Eerste fase evaluatie
Wet bescherming persoonsgegevens

Literatuuronderzoek en knelpuntenanalyse

Gerrit-Jan Zwenne, Anne-Wil Duthler, Marga Groothuis,
Hugo Kielman, Wouter Koelewijn en Laurens Mommers

eLaw@Leiden, Centrum voor
Recht in de Informatiemaatschappij
Postbus 9520 2300 RA Leiden

in samenwerking met

Afdeling Staats- en Bestuursrecht
Universiteit Leiden
Postbus 9520 2300 RA Leiden

en

Duthler Associates
Frankenslag 137
2582 HH Den Haag

Inhoud

Samenvatting

Dit rapport betreft de eerste fase van de evaluatie van de Wet bescherming persoonsgegevens (Wbp), zoals bedoeld in artikel 80 Wbp. Allereerst is geïnventariseerd wat de doelstellingen waren bij de invoering van de Wbp. Daarnaast is – voorzover deze doelstellingen samenhangen met de implementatie van de privacy-richtlijn 95/46/EG – nagegaan wat de bedoelingen van de gemeenschapswetgever daarbij waren (doelstellingeninventarisatie). Vervolgens is onderzocht welke knelpunten er in de literatuur en rechtspraak zijn gesignaleerd bij de uitvoering en toepassing van de wet (knelpuntenanalyse). Het doel van dit onderzoek is het doen van aanbevelingen met betrekking tot het nader articuleren van de onderzoeksvragen voor de tweede fase van de evaluatie (vraagarticulatie).

De Wbp vormt de implementatie van de privacy-richtlijn 95/46/EG in de Nederlandse rechtsorde. Daarom is in het eerste deel van de doelstellingeninventarisatie gekeken naar de bedoelingen van de gemeenschapswetgever (hoofdstuk 2). Met de richtlijn beoogt de gemeenschapswetgever bij te dragen aan de verwezenlijking van de algemene doelstellingen van de Gemeenschap door enerzijds een bijdrage te leveren aan de totstandbrenging en werking van de interne markt en anderzijds waarborgen te bieden voor de bescherming van fundamentele rechten en vrijheden. De bijdrage aan de interne markt is gelegen in het wegnemen van marktbelemmeringen die kunnen voortvloeien uit de verschillen tussen nationale wettelijke regimes voor de verwerking van persoonsgegevens. De gemeenschapswetgever heeft daarom gekozen voor een ruime werkingssfeer van de richtlijn die met name, maar niet uitsluitend, ziet op geautomatiseerde verwerkingen. Ter waarborging van fundamentele rechten en vrijheden beoogt de richtlijn via harmonisering van wetgeving te komen tot een gelijkwaardig en hoog beschermingsniveau voor alle lidstaten. In verband met de totstandbrenging van een hoog beschermingsniveau verwijst de richtlijn naar het EVRM en de privacybeginselen die zijn neergelegd in het Verdrag inzake gegevensbescherming. Verder moet het hoge beschermingsniveau worden bereikt door de transparantie van gegevensverwerkingen te verbeteren en te voorzien in waarborgen voor betrokkenen. Om te komen tot een gelijkwaardig beschermingsniveau beoogt de richtlijn de nationale privacywetten van lidstaten met elkaar in overeenstemming te brengen en ervoor te zorgen dat in de verschillende lidstaten soortgelijke aanspraken en verplichtingen gelden ten aanzien van de bescherming van persoonsgegevens.

De gemeenschapswetgever heeft met de richtlijn ten slotte ook tegemoet willen komen aan de bijzonderheden van bepaalde categorieën van gegevens of verwerkingen. Daarom biedt zij de nationale wetgever in aangegeven gevallen 'een zekere bandbreedte'. Die flexibiliteit komt mede tot uitdrukking in de doelstelling om zoveel mogelijk rekening te houden met de specifieke omstandigheden en behoeften van een sector of branche. Daartoe voorziet de richtlijn in de mogelijkheid dat op branche- en sectorniveau gedragscodes worden opgesteld.

In het tweede deel van de doelstellingeninventarisatie is geïnventariseerd welke bedoelingen de nationale wetgever heeft gehad met invoering van de Wbp (hoofdstuk 3). Daarbij is een onderscheid gemaakt tussen de formele en materiële doelstellingen van de Wbp. De formele doelstellingen vloeien voort uit de verplichtingen waaraan de wetgever gebonden is op grond van hogere regelgeving zoals het EG-verdrag en de privacy-richtlijn. De materiële doelstellingen zien op de wijze waarop de formele doelstellingen zijn gerealiseerd.

De eerste formele doelstelling van de Wbp is de implementatie van de richtlijn en het verder invulling geven aan de voorwaarden waaronder verwerkingen rechtmatig zijn. Daarbij is het de bedoeling van de nationale wetgever dat een nadere concretisering van de normen uit de Wbp moet plaatsvinden in sectorale wetgeving en zelfregulering, alsmede in de jurisprudentie. De tweede formele doelstelling betreft het uitvoering geven aan de opdracht van de grondwetgever om regels te stellen in verband met de vastlegging

en verstrekking van persoonsgegevens. De derde formele doelstelling ten slotte is het uitvoering geven aan het Verdrag inzake gegevensbescherming en het aan sluiten bij de relevante jurisprudentie van het EHRM.

Wat betreft de materiële doelstellingen beoogt de Wbp allereerst de waarborgen te bieden waarmee een evenwicht tussen privacybescherming en andere grondrechten wordt bewerkstelligd. De wetgever heeft ervoor gekozen om daarbij gebruik te maken van open normen, omdat op die manier wordt voorzien in een instrumentarium met behulp waarvan steeds een afweging mogelijk is van de bij de gegevensverwerkingen betrokken belangen. De wetgever acht het in dat verband van belang dat de Wbp goed is ingebed in het rechtsstelsel en aansluit bij de bestaande jurisprudentie.

Verder ziet de Wbp op het versterken van de positie van de betrokkenen door het verantwoordelijkebegrip te verhelderen en de transparantie van gegevensverwerkingen te vergroten. De wet doet dit door rechten toe te kennen aan betrokkenen en daarmee corresponderende verplichtingen op te leggen aan verantwoordelijken. Voor het toezicht en de controle op de naleving van de wet is het College bescheming persoonsgegevens (Cbp) ingesteld. Naast deze centrale toezichthouder voorziet de wet ook in de mogelijkheid tot het aanstellen van een Functionaris Gegevensbescherming (FG). Daarmee wordt beoogd de kennisontwikkeling over gegevensbescherming en het privacybewustzijn bij verantwoordelijken te bevorderen. Ook de meldplicht kan worden gezien als een middel om zelfregulering op het niveau van de verantwoordelijke te stimuleren.

Bij de knelpunteninventarisatie zijn op basis van het literatuuronderzoek eerst de meest in het oog springende algemene knelpunten met betrekking tot de toepassing en uitvoering van de Wbp in kaart gebracht (hoofdstuk 4). Een aantal auteurs ziet ten eerste de onduidelijkheid en onbepaaldheid van de wettelijke begrippen als een knelpunt, omdat zij de naleving van de wet belemmeren en in de weg kunnen staan aan technologische ontwikkeling en innovatie. Andere auteurs pleiten daarentegen juist voor het behoud van de brede werkingssfeer.

In de literatuur wordt verder gewezen op knelpunten die voortvloeien uit het algemene, omnibuskarakter van de wet. Het gaat dan met name om de ingewikkeldheid en de inflexibiliteit van de wet. Daartegenover staat dat een enkele andere auteur meent dat een omnibus juist noodzakelijk is om alle betrokken belangen in hun onderlinge samenhang te kunnen bezien. Bij de in het kader van dit onderzoek geraadpleegde domeindeskundigen bleek er weinig draagvlak te zijn voor een sectorale benadering in plaats van de huidige omnibusbenadering.

In de literatuur zijn daarnaast knelpunten gesignaleerd waar het gaat om het vaststellen van wie de verantwoordelijke is op wie de materiële normen van de wet primair van toepassing zijn. Deze problemen doen zich in het bijzonder voor bij samenwerkingsverbanden, joint venture-constructies, en in de context van internet. Volgens sommige auteurs heeft de wet een eenzijdig procedureel karakter en biedt hij te weinig harde materiële normen. Volgens andere auteurs is de wet te onpraktisch omdat deze ervan uit gaat dat bij elke verwerking aan de (te vage) normen van de Wbp wordt getoetst. Ook is er kritiek op het aanduiden van een hele categorie van gegevens als bijzondere gegevens. Dit leidt in de praktijk tot knelpunten omdat de gevoeligheid van bijzondere gegevens contextafhankelijk is.

Waar het gaat om de totstandkoming van gedragscodes wordt door enkele auteurs de invloed die het Cbp heeft op grond van zijn goedkeuringsbevoegheid gezien als knelpunt. Het opstellen van gedragscodes is volgens hen een langdurig, tijdrovend en kostbaar proces waar maar weinig concrete voordelen tegenover staan. Ook worden in de literatuur vraagtekens geplaatst bij de waarborging van de onafhankelijkheid van de FG. Vanuit de beroepsvereniging voor FG's wordt er wel op aangedrongen dat in de private sector meer FG's worden aangesteld. Ook ten aanzien van de bijdrage van de FG's aan de vergroting van de transparantie van verwerkingen zijn de meningen verdeeld. In de literatuur is er discussie over de vraag of het Cbp voldoende of juist te weinig bevoegdheden heeft. Daarbij wordt gewezen op knelpunten met betrekking tot de naleving van de wet en knelpunten op het gebied van de handhaving. In het verlengde

daarvan worden ook kritische kantekeningen geplaatst bij het systeem van rechtsbescherming. Aan de verschillende bestuurs- en civielrechtelijke procedures zijn nadelen verbonden, zoals forumshopping. Ook kunnen de verschillende rechterlijke competenties afbreuk doen aan de rechtseenheid.

Als het gaat om internationale doorgifte van persoonsgegevens wordt vooral het vergunningvereiste ervaren als een knelpunt. Dat geldt in het bijzonder voor de doorgifte van persoonsgegevens van een vestiging van een verantwoordelijke binnen de EU naar een vestiging van de verantwoordelijke daarbuiten. Deze 'interne' doorgifte valt niet onder de uitzonderingen op het doorgifteverbod. Ook wordt gepleit voor een administratieve lastenverlichting door het afschaffen van de vergunningsplicht wanneer gebruik wordt gemaakt van daarvoor bestemde modelcontracten.

In de private sector (hoofdstuk 5) worden met betrekking tot het begrippenapparaat van de Wbp vooral knelpunten geconstateerd bij multinationale ondernemingen. Met name de onduidelijkheden en onbepaaldheid van belangrijke begrippen, zoals persoonsgegevens, verwerking, verantwoordelijke en bewerker, geven aanleiding tot problemen bij internationale gegevenstromen, fusies en overnames.

Ook worden in de literatuur knelpunten gesignaleerd met betrekking tot de aansluiting van de Wbp met andere wetgeving, zoals de Databankenwet en de Aanpassingswet inzake richtlijn elektronische handel. Een verschil in gebruik van de begrippen leidt daar tot verwarring. Andere toepassingsproblemen hangen samen met de formulering van het normatieve kader van de Wbp. Dit heeft in de private sector tot gevolg dat de Wbp niet in alle gevallen een duidelijk beeld geeft van wat wel kan en wat niet. Uit literatuur blijkt dat er in ieder geval knelpunten in de private sector bestaan ten aanzien van het begrip 'toestemming' en het 'gerechtvaardigd belang', en de (on)rechtmatige toegang tot (bijzondere) gegevens door derden.

Een belangrijke doelstelling van de Wbp betreft de transparantie en de versterking van de positie van betrokkenen. Uit de literatuur komt het beeld naar voren dat er in de private sector knelpunten zijn bij het melden van een gegevensverwerking en de onmogelijkheid om gebruik te kunnen maken van een in het Vrijstellingsbesluit opgenomen vrijstelling op de meldplicht. Het gaat dan om het als lastig getypeerde elektronisch meldingssysteem; het vanwege de gedetailleerdheid onwerkbare vrijstellingsbesluit, en een, als direct gevolg van de melding, verplichte openbaarheid van de gegevensverwerkingen. Verder laat de literatuur zien dat er knelpunten zijn bij het vormgeven en naleven van de informatieplicht. Het vooraf informeren van betrokkenen is arbeidsintensief en botst in sommige gevallen met het vertrouwelijke karakter van de betreffende gegevensverwerking. Daarnaast wordt de informatieplicht als lastig toepasbaar ervaren door het gebruik van open normen. Met betrekking tot de rechten van betrokkenen zijn er onduidelijkheden rond de reikwijdte van het kennisnemingsrecht, dat vooral vorm heeft gekregen in de Dexia-zaken.

Tegen bepaalde beslissingen van de verantwoordelijke kan een belanghebbende zich tot de rechtbank wenden. In literatuur wordt een aantal knelpunten gesignaleerd dat met deze 'nieuwe' civiele rechtsgang te maken heeft. Er wordt gewezen op de onbekendheid bij rechters met de Wbp en de niet eenduidigheid en hoogdrempeligheid van de civiele procedure. Controle en toezicht op de gegevensverwerkingen in de private sector is in eerste instantie een taak van het Cbp. Deze lijkt geneigd te zijn om meer gebruik te willen maken van een actief publicatiebeleid in het kader van zijn toezichthoudende taken, het zogenoemde 'naming and shaming'.

De literatuur laat met betrekking tot de publieke sector (hoofdstuk 6) soortgelijke knelpunten zien als in de private sector geconstateerd zijn. Zo bestaan ook in de publieke sector onduidelijkheden over de uitleg en toepassing van begrippen als verantwoordelijke en persoonsgegeven, alsmede over de verhouding tussen de Wbp en andere wetten, zoals de Wob en de WBibob. Vooral de aanwezigheid van tal van sectorale regelgeving omtrent het gebruik van persoonsgegevens (zoals WGBA en de Wpolr) is kenmerkend voor de publieke sector. Dit beperkt de werkingssfeer van de Wbp in deze sector.

Als het gaat om de normatieve kaders doen zich in de publieke sector knelpunten voor ten aanzien van het verbod van verwerken van bijzondere gegevens. Dit geldt met name bij het controleren van de naleving van wetgeving waarvoor bijzondere gegevens als gezondheidsgegevens worden bijgehouden.

Met betrekking tot het thema zelfregulering valt op dat in de publieke sector relatief veel FG's aangesteld zijn, maar dat er geen sprake is gedragscodes. Wel is er sprake van informele zelfregulering, zoals netwerken of platforms waarbinnen afspraken worden gemaakt over gegevensverwerkingen of bijvoorbeeld best practices worden uitgewisseld.

Van het kennisnemings- en correctierecht lijkt in de publieke sector in het algemeen niet veel gebruik te worden gemaakt. Er zijn aanwijzingen dat procedures en maatregelen ontbreken om deze rechten binnen de wettelijke termijnen op een zorgvuldige wijze te kunnen effectueren.

Met betrekking tot het onderwerp toezicht en rechtsbescherming zijn er in de literatuur een aantal specifieke knelpunten gesignaleerd in de publieke sector. De doorlooptijd van het voorafgaand onderzoek, dat door het Cbp in bepaalde gevallen verplicht wordt uitgevoerd, kan een knelpunt vormen, in het bijzonder voor samenwerkingsverbanden. De uitoefening van het toezicht door FG's levert in de publieke sector nauwelijks knelpunten op. Dat geldt niet voor de rechtsbescherming, die in de publieke sector anders is geregeld dan in de private sector. Dit komt volgens sommige auteurs de rechtseenheid en de privacybescherming niet ten goede.

Ook in de semi-publieke sector (hoofdstuk 7) leiden een aantal kernbegrippen tot problemen. Zo brengt de onbepaaldheid van het begrip persoonsgegeven onduidelijkheid met zich mee over de reikwijdte van de wet en leidt dit tot uiteenlopende interpretaties. Als onduidelijk worden gezien de begrippen verantwoordelijke en bewerker. Ook wordt wel aangegeven dat de toepassing van de Wbp in de semi-publieke sector wordt belemmerd door een veelheid aan sectorale regelingen. In combinatie met het hoge abstractieniveau van de Wbp leidt dit tot een ondoorgrondelijk regelstelsel. Daarnaast wordt de Wbp in de praktijk als belemmerend ervaren bij de uitvoering van beleid waarin toegewerkt wordt naar een 'klantvriendelijke' dienstverlening en waarin het de bedoeling is dat slechts één keer gegevens worden opgevraagd van de burger. In verband daarmee blijkt uit de literatuur dat er bij hulpverleners in samenwerkingsverbanden en ketenzorg onbekendheid is met de interpretatieruimte van de Wbp. Deze onbekendheid heeft in sommige gevallen tot gevolg dat er door hulpverleners onterecht vanuit wordt gegaan dat bepaalde gegevensverwerkingen niet zijn toegstaan. De normatieve kaders van de Wbp roepen in de semi-publieke sector een aantal specifieke vragen op. Bijvoorbeeld in de zorg- en hulpverlening. Daar waar zonder de instemming van de betrokkene wordt gehandeld werpt de Wbp belemmeringen op.

Met betrekking tot het thema zelfreguling blijkt dat de gedragscode die van toepassing is op zorgverzekeraars de regeldichtheid vergroot, maar niet voldoende in staat is adequaat te reageren op nieuwe ontwikkelingen binnen de zorgsector. Waar het gaat om de transparantiedoelstelling en de rechten van betrokkenen, worden in de semi-publieke sector soortgelijke knelpunten gesignaleerd als in de overige sectoren. De effectuering van het kennisnemingsrecht bij zowel de betrokkene als de verantwoordelijke wordt belemmerd door een aantal praktische problemen die worden gezien als gevolg van het hoge abstractieniveau en te rigide normstelling in het zgn. Kostenbesluit. Verder zijn er signalen dat de informatieplicht en het toestemmingsvereiste bij 'grote' uitvoeringsorganisaties zorgen voor relatief hoge uitvoeringskosten.

In de rechtspraak en literatuur worden weinig knelpunten gesignaleerd die specifiek betrekking hebben op de rechtsbescherming, handhaving en toezicht binnen de semi-publieke sector. De verschillende wetgevingsadviezen en uitspraken van het Cbp wekken de indruk dat het toezicht op, en de handhaving van de wet goed zijn geregeld. Wel wordt in dit verband gewezen op het gevaar van pseudowetgeving. Met betrekking tot de rechtsbescherming vormt de onbekendheid en de daarmee samenhangende verkeerde toepassing van het verzetsrecht het meest in het oogspringende knelpunt.

Ten slotte is aan de hand van de knelpunteninventarisatie nagegaan in hoeverre de doelstellingen van Wbp en voorzover relevant, van de richtlijn zijn gehaald (hoofdstuk 8). Daarvoor zijn de verschillende knelpunten die in de literatuur zijn gesignaleerd, gekoppeld aan de doelstellingen van de Nederlandse wetgever. Vervolgens zijn de belangrijkste conclusies bezien vanuit drie beoordelingsperspectieven.

Ten eerste kan vanuit het juridisch perspectief worden gewezen op de belangrijkste knelpunten die voortvloeien uit de moeizame aansluiting van de Wbp bij het Nederlandse rechtssysteem. Het gelaagde en gecompartimenteerde systeem voor de bescherming van persoonsgegevens is bijzonder complex geworden en tendeert soms zelfs naar overregulering. Daar komt bij dat het begrippenapparaat en instrumentarium van de Wbp als zodanig te abstract zijn en te veel ruimte laten voor interpretatie om een helder kader te vormen voor de beoordeling van concrete vragen en situaties. Daarmee wordt de doelstelling van het vaststellen van een begrippenapparaat dat bruikbaar is voor rechtsvorming en voor de afweging van belangen niet (ten volle) gerealiseerd.

Ten tweede kan vanuit het perspectief van de handhaving en de naleving worden gewezen op het eenzijdig karakter van de handhaving doordat de nadruk vooral ligt op de doorgaans gevolgde bestuursrechtelijke rechtsgang. Daarnaast krijgt het beoogde stelsel van checks and balances maar beperkt vorm door het gebrek aan feitelijke rechterlijke toetsing van de beginselen uit de Wbp. Verder laat de zelfregulering in het kader van de Wbp te wensen over. Ook kan worden geconcludeerd dat in het bijzonder de doelstellingen van de rechterlijke toetsing van de aan het Cbp toegekende bevoegdheden, en de nadere invulling van materiële normen via zelfregulering, maar beperkt gerealiseerd zijn.

Ten derde valt vanuit het perspectief van de beeldvorming en bekendheid op dat veel rechten en plichten van verantwoordelijken en betrokkenen die voortvloeien uit de Wbp, niet optimaal worden uitgeoefend door een gebrek aan bekendheid van deze rechten en plichten. Een van de centrale doelstellingen van de Wbp, namelijk het vergroten van de transparantie van gegevensverwerking door de toekenning van rechten en plichten en het instellen van een toezichthouden lijkt daarmee (ten dele) onwerwezenlijkt. Tot slot vormt het overzicht vanuit de drie perspectieven het uitgangspunt voor de bepaling van relevante vragen voor de tweede fase van de evaluatie waarin een empirische onderzoek gedaan zal worden naar de doeltreffendheid van de Wbp.

Hoofdstuk 1: Inleiding

1.1 Inleiding

Dit rapport betreft een literatuurstudie waarin wordt geïnventariseerd in hoeverre en op welke wijze de Wet bescherming persoonsgegevens (Wbp) een bijdrage heeft geleverd aan het realiseren van de doelstellingen van deze wet, alsmede welke knelpunten zich in de praktijk hebben voorgedaan bij de uitvoering en toepassing daarvan. Het onderzoek heeft dan ook een beschrijvend karakter. Het beschrijft welke doelstellingen de wetgever had met de wet en mede in verband daarmee welke knelpunten in de literatuur zijn gesignaleerd en geïdentificeerd bij de toepassing van de wet in de praktijk. Dit betekent dat het onderzoeksveld is gericht op het aangeven van wat in de literatuur over de wet als problematisch wordt aangemerkt, en niet zozeer op wat als probleemloos wordt gezien. Ook betekent dit dat het onderzoeksveld is beperkt tot wat uit openbaar toegankelijke bronnen kenbaar is.

Deze literatuurstudie vindt plaats in het kader van de evaluatie van de wet, zoals die is voorzien in artikel 80 Wbp. De eerste fase van deze evaluatie, waarvan dit rapport verslag doet, is bedoeld om inzicht te krijgen in de belangrijkste evaluatiepunten (knelpunten en discussiepunten) van de Wbp. De in de literatuurstudie gevonden evaluatiepunten worden vervolgens gebruikt als bouwstenen voor de nadere invulling van de tweede fase van het evaluatieonderzoek, dat meer empirisch georiënteerd is.

1.2 Aanleiding en doelstelling van het onderzoek

Artikel 80 Wbp verlangt dat de Staten Generaal binnen vijf jaren na inwerkingtreding van de wet worden geïnformeerd over de doeltreffendheid en de effecten van deze wet in de praktijk. Daarbij gaat het om het in kaart brengen van de wettelijke bepalingen die knelpunten opleveren of in onvoldoende mate waarborgen bieden voor de bescherming van de persoonlijke levenssfeer.[1] Om uitvoering te geven aan deze evaluatiebepaling heeft het Ministerie van Justitie, mede namens het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, opdracht gegeven tot een evaluatieonderzoek.

Omdat de reikwijdte van de wet groot is wordt dit evaluatieonderzoek in twee fasen uitgevoerd. De eerste fase, waarvan dit rapport verslag doet, betreft een literatuurstudie op hoofdlijnen. Op basis van een analyse van de parlementaire geschiedenis worden de doelstellingen van de wet uiteengezet, waarna mede in verband daarmee aan de hand van literatuur de belangrijkste knelpunten en discussiepunten in kaart worden gebracht. Op basis daarvan worden aanbevelingen gedaan voor de invulling en opzet van het tweede fase onderzoek, dat voortbouwt op de resultaten van dit eerste fase onderzoek en een meer empirisch sociologisch deel omvat dat zal ingaan op de kenbaarheid en werking van de wet in de praktijk. In deze tweede fase worden de geïdentificeerde knelpunten getoetst aan de praktijk

1.3 Probleem- en vraagstelling, en opzet

De probleemstelling van het evaluatieonderzoek is afgeleid van artikel 80 Wbp, de evaluatiebepaling in de wet. Verwoord als een drieledige vraag luidt deze probleemstelling als volgt:

- op welke wijze draagt de Wbp bij aan de door de wetgever beoogde doelstellingen, gegeven de normstelling en de reikwijdte van de wet?

---

[1] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 197.

- in hoeverre sluit de wet aan bij overige wetgeving?
- en welke knelpunten doen zich voor in de praktijktoepassing van de wet?

Om te komen tot een beantwoording van deze vragen wordt in deze eerste fase van het evaluatieonderzoek enerzijds nagegaan wat volgens de parlementaire geschiedenis en andere achtergrondstukken de doelstellingen van de wet waren en op welke wijze de wetgever deze beoogde te realiseren (doelstellingeninventarisatie); anderzijds wordt nagegaan welke knelpunten er in literatuur en rechtspraak worden geïdentificeerd bij de toepassing van de wet, alsmede welke oplossingsrichtingen worden gesuggereerd (knelpuntenanalyse). Vervolgens worden op basis van de uitkomsten daarvan aanbevelingen gedaan voor de opzet en van de tweede fase van het evaluatieonderzoek (vraagarticulatie).

1.3.1 Doelstellingeninventarisatie

In de doelstellingeninventarisatie wordt nagegaan wat de doelstellingen van de wetgever waren met de Wbp, en voorzover deze samenhangen met de implementatie van de privacy-richtlijn 95/46/EG[2] (de privacy-richtlijn) wat de bedoelingen van de gemeenschapswetgever daarbij waren. De belangrijkste bronnen voor dit onderdeel van de literatuurstudie zijn dan ook de privacy-richtlijn en de parlementaire geschiedenis van de Wbp. Daarnaast worden ook inzichten ontleend aan het Implementatierapport van de Europese Commissie uit 2003, waarin wordt aangegeven wat er (nog) niet goed is geregeld. In dat verband komt ook betekenis toe aan de opmerkingen van een aantal lidstaten, waaronder in een later stadium Nederland, voor aanpassing van de privacy-richtlijn. Hetzelfde geldt voor de inbreng van Nederlandse maatschappelijke organisaties in de consultatie voorafgaand aan dit Implementatierapport.

De privacy-richtlijn en daarmee de Wbp kunnen niet los worden gezien van de ontwikkeling van de informatiemaatschappij en de economische groei die deze mogelijk maakt. Om deze reden, maar niet alleen daarom, ligt het voor de hand om ook enige aandacht te besteden aan de bijdrage die de wet heeft geleverd aan deze economische ontwikkeling. Daarvoor is onder andere gebruik gemaakt van de economische evaluatie van de richtlijn die vorig jaar in opdracht van de Europese Commissie is verricht.[3]

1.3.2 Knelpuntenanalyse

In de knelpuntenanalyse wordt nagegaan welke knelpunten er in literatuur en rechtspraak worden geïdentificeerd bij de toepassing van de wet, en welke oplossingsrichtingen worden gesuggereerd. In dit onderdeel van de literatuurstudie wordt uitgegaan van de systematiek zoals neergelegd in de hoofdstukindeling van de wet en de richtlijn. Aan de hand van deze hoofdstukken kunnen zes thema's worden onderscheiden die worden gebruikt bij de ordening en analyse van de te inventariseren knelpunten.

De onderscheiden thema's zijn de volgende: (1) werkingssfeer en toepassing, (2) normatieve kaders, (3) zelfregulering, (4) transparantie en rechten van betrokkenen, (5) rechtsbescherming, handhaving en toezicht, en (6) internationale gegevensdoorgifte. De thema's corresponderen met de belangrijkste hoofd-

---

[2] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PbEG* L 281 van 23/11/1995, p. 0031 – 0050.
[3] Zie m.n. paragrafen 2.2 en 3.3.6.

stukken uit de wet en de richtlijn.[4] De relatie tussen de thema's, hoofdstukken en wettelijke bepalingen is in onderstaand overzicht uiteengezet.

Thema's	**Wet bescherming persoonsgegevens**		
1. werkingssfeer en toepassing	Hoofdstuk 1	algemene bepalingen	art. 1-5
2. normatieve kaders	Hoofdstuk 2	voorwaarden voor de rechtmatigheid van verwerkingen	art. 6-24
	Hoofdstuk 7	uitzonderingen en beperkingen	art. 43
3. zelfregulering	Hoofdstuk 3	gedragscodes	art. 25-26
	Hoofdstuk 9	functionaris voor de gegevensbescherming	art. 62-64
4. transparantie en rechten van betrokkenen	Hoofdstuk 4	melding	art. 27-30
	Hoofdstuk 5	informatieverstrekking aan betrokkenen	art. 33-34
	Hoofdstuk 7	uitzonderingen en beperkingen	art. 43-44
	Hoofdstuk 4	informatie op verzoek	art. 30 lid 3
	Hoofdstuk 6	rechten van betrokkenen	art. 35-42
	Hoofdstuk 7	uitzonderingen en beperkingen	art. 43-44
5. rechtsbescherming, handhaving en toezicht	Hoofdstuk 4	voorafgaand onderzoek	art. 31-32
	Hoofdstuk 8	rechtsbescherming	art. 45-50,
	Hoofdstuk 9	toezicht	art. 51-64
	Hoofdstuk 10	sancties	art. 65-75
6. internationale gegevensdoorgifte	Hoofdstuk 11	gegevensverkeer met landen buiten de EU	art. 76-78

In aanvulling daarop kunnen nog twee thema's worden onderscheiden die niet direct een relatie hebben met hoofdstukken uit de wet of richtlijn, maar waaraan bij de voorbereiding van de wet zoveel aandacht is besteed dat deze in aanmerking komen voor een afzonderlijke bespreking. Het gaat dan om de uitvoeringskosten of administratieve lasten en de technologie-onafhankelijkheid van de wet.

Aanvullende thema's
7. uitvoeringskosten
8. technologie-onafhankelijkheid

Uitgaande van deze thema's is telkens aan de hand van literatuur en rechtspraak in kaart gebracht welke belangrijkste, meest in het oogspringende knelpunten er zijn geïdentificeerd. Vanwege het sectoroverschrijdende karakter van de Wbp is allereerst gekozen voor een overzicht van de algemene knelpunten gevolgd door een bespreking van knelpunten die specifiek samenhangen met de private, publieke en semi-publieke sector. In dat verband wordt onder publieke sector verstaan: de ministeries, de decentrale overheden, de openbare lichamen en zelfstandige bestuursorganen met rechtspersoonlijkheid die bij of krachtens de wet is ingesteld. Onder semi-publieke sector wordt verstaan de privaatrechtelijke rechtspersonen

[4] Met uitzondering van hoofdstuk 12 van de Wbp waarin de overgangs- en slotbepalingen staan opgenomen die betrekking hebben op overgangstermijnen (art. 79), de evaluatie van de wet (art. 80), intrekking van de Wet persoonsregistraties (art. 81), inwerkingtreding (art. 82) en de citeertitel (art. 83). Deze bepalingen lenen zich niet voor het onderhavige evaluatieonderzoek en worden daarom niet in het literatuuronderzoek betrokken.

die volledig of in aanzienlijke mate worden gefinancierd uit publieke middelen of waarvan de financiering tot de collectieve lasten wordt gerekend, zoals instellingen in de zorg- en onderwijssector, de publieke omroepen en de verschillende uitvoeringsinstanties in de sociale zekerheid.[5] Onder de private sector wordt dan alles verstaan wat niet onder de publieke en semi-publieke sector valt.

Buiten de kaders van dit onderzoek vallen vragen die specifiek raken aan het thema 'privacy en veiligheid', dat onderwerp is van een separaat onderzoek.[6] Ook het intern functioneren van de toezichthouder, het College bescherming persoonsgegevens (Cbp) valt buiten het bereik van het onderzoek. Wel is er aandacht gegeven aan de uitspraken, oordelen, achtergrondstudies en andere documenten van de teozichthouder.

1.3.3 Vraagarticulatie

In het onderdeel vraagarticulatie worden op basis van de resultaten van de doelstelling- en knelpuntenanalyse aanbevelingen en suggesties gedaan voor de opzet en invulling van de tweede fase van het evaluatieonderzoek, dat een meer empirische karakter zal hebben en dat vooral zal ingaan op de kenbaarheid en werking van de wet in de praktijk. De in dit onderdeel beantwoorde vragen zijn de volgende:

- wat zijn de meest voor de hand liggende operationaliseerbare grootheden voor het meten van de doeltreffendheid van de Wbp?
- welke methoden dienen te worden ingezet voor de beantwoording van de onderzoeksvragen van de tweede fase?

Om deze vragen te beantwoorden zijn de bevindingen van de knelpuntenanalyse gepresenteerd vanuit het perspectief van drie invalshoeken, te weten een formeel-juridische invalshoek, de invalshoek van naleving en handhaving, en de invalshoek van beeldvorming en bekendheid,

Vanuit de juridische invalshoek is gekeken naar de belangrijkste juridische knelpunten van de Wbp. Het gaat daarbij onder meer om complicaties in verband met de open normstelling in de wet, de interpretatie van kernbegrippen door verschillende rechters, inconsistenties in de wet en in verhouding met andere wetten, alsmede de inbedding van de wet in andere rechtsgebieden en jurisdictievraagstukken verband houdend met internationalisering en grensoverschrijdend gegevensverkeer.

Vanuit de invalshoek van naleving en handhaving is gekeken naar de houdbaarheid en werkzaamheid van de Wbp in een omgeving van technologische turbulentie, de in de literatuur geconstateerde feitelijke realisatie van de bescherming van persoonsgegevens, en de inventarisatie van de belangrijkste beleidsmatige en uitvoeringsgerelateerde resultaten en knelpunten, zoals de administratieve lasten die samenhangen met de Wbp.

Vanuit de invalshoek van de beeldvorming en bekendheid is ten slotte gekeken naar de gerealiseerde perceptie en bewustwording van de bescherming van persoonsgegevens. Het gaat daarbij om de gevoelens bij het publiek over de mate waarin hun gegevens en de persoonlijke levenssfeer door de Wbp worden beschermd, kennis bij relevante organisaties en personen en het daadwerkelijke gebruik van kennisnemingen verbeteringsrechten.

---

[5] Vgl. Voorstel voor Wet openbaarmaking uit publieke middelen gefinancierde topinkomens. *Kamerstukken II* 2004-2005*,* 30 189, nr. 3, p. 5.
[6] Dit onderzoek wordt uitgevoerd door het Molengraaff Instituut te Utrecht.

1.4 Werkwijze en verantwoording

De studie waarvan dit rapport verslag doet betreft een literatuuronderzoek en is dus descriptief van aard. In het onderzoek is geïnventariseerd wat er in de literatuur over de Wbp is gezegd over de doelstellingen en knelpunten van de wet. Waar het gaat om de doelstellingen van de wet is is daarbij vooral uitgegaan van de parlementaire geschiedenis van de wet, alsmede van achtergrondstukken van de privacyrichtlijn die door de wet wordt geïmplementeerd. Voor het identificeren van knelpunten is allereerst uitgegaan van de literatuur die is gericht op het privacy- en gegevensbeschermingsrecht, zoals het tijdschrift *Privacy & Informatie* en de handboeken op dit gebied.[7] Verder is uitgegaan van specifieke publicaties, zoals enkele proefschriften en de onderzoeksrapporten die zijn gepubliceerd in het kader van het onderzoeksprogramma IT en Recht (ITeR). In aanvulling op de tijdschriften waarin vanouds ook veel wordt geschreven over privacy en gegevensbescherming, zoals de *Computerrecht* en *Mediaforum*, zijn in de literatuurstudie ook publicaties van het College bescherming persoonsgegevens betrokken, alsmede bijdragen over de Wbp in tijdschriften als *Arbeidsrecht*, *Sociaal recht*, *Tijdschrift voor financieel recht* en dergelijke.

Er is evenwel veel meer over de Wbp geschreven dan binnen de beperkingen van dit onderzoek kan worden verwerkt. Het is dan ook onvermijdelijk dat de literatuurstudie een selectie betreft waarbij keuzes zijn gemaakt die in meer of minder mate arbitrair kunnen worden gevonden. Om deze keuzes op een zo verantwoord mogelijke wijze te maken en om te voorkomen dat belangrijke elementen werden gemist, is op verschillende momenten in het onderzoek gebruik gemaakt van de beschikbare kennis en ervaring uit het werkveld. Zo zijn aan het begin van het onderzoek drie diepte-interviews gehouden met deskundigen die zich vanuit hun eigen expertise al langere tijd bezighouden met de wet. In de loop van het onderzoek de voorlopige bevindingen voorgehouden aan zgn. domeindeskundigen, ofwel mensen die van dichtbij kennis hebben van de knelpunten die zich daarbij in de praktijk voordoen, zoals functionarissen voor de gegevensbescherming, privacyfunctionarissen, privacyadviseurs en dergelijke. In aanvulling daarop is er ten slotte nog een gesprek geweest met enkele deskundigen die betrokken waren bij het wetgevingsproces en/of meer met een helicopter-view inzichten daarover hebben ontwikkeld.[8]

Deze gesprekken en bijeenkomsten zijn gebruikt om het onderzoek richting te geven en om de bevindingen te reflecteren. De resultaten ervan zijn gebruikt om het onderzoek in de aangegeven richting uit te werken of te verdiepen, teneinde een adequaat beschrijving te geven van wat in de literatuur is gezegd over de realisatie van de doelstellingen van deze wet en de knelpunten zich in de praktijk hebben voorgedaan bij de uitvoering en toepassing daarvan.

Op deze wijze wordt beoogd een zo volledig mogelijk beeld te geven van wat er in de literatuur is gezegd over de werking van de Wbp. Maar zoals bij alle literatuurstudies gelden daarbij beperkingen. Het is enerzijds niet uitgesloten dat er zich in de praktijk knelpunten voordoen die niet in de literatuur zijn gesignaleerd of geïdentificeerd, en die dus niet of beperkt in het onderzoek naar voren komen. Anderzijds is het denkbaar dat er aan de knelpunten die wel in de literatuur zijn geïdentificeerd om wat voor reden dan ook in die literatuur onevenredig veel aandacht is gegeven. Om een evenwichtig en representatief beeld te krijgen is dan ook een nadere 'reality check' nodig. Daarin voorziet het tweede fase-onderzoek, dat zoals gezegd meer empirische componenten bevat.

---

[7] O.a. Berkvens & Prins 2002.

[8] Zie voor een overzicht van de verschillende bijeenkomsten en personen die daaraan hebben deelgenomen Bijlage A bij dit rapport.

1.5 Structuur van dit rapport

De structuur van dit rapport komt overeen met de in het voorgaande uiteengezette werkwijze en opzet van het onderzoek.

In hoofdstuk 2 wordt verslag gedaan van het eerste deel van de doelstellingenanalyse. In dit hoofdstuk wordt nagegaan wat de doelstellingen van de gemeenschapswetgever waren met de richtlijn, die door de wetgever is geïmplementeerd door middel van de Wbp.

In hoofdstuk 3 wordt in aansluiting daarop verslag gedaan van het tweede deel van de doelstellingenanalyse. In dit hoofdstuk wordt nagegaan wat de doelstellingen waren van de nationale wetgever met de Wbp.

In hoofdstuk 4 wordt het eerste deel van de knelpuntenanalyses uitgevoerd. Er wordt vanuit de zes onderscheiden thema's geïnventariseerd wat de belangrijkste en meest in het oogspringende knelpunten zijn. Dit hoofdstuk betreft de algemene, dus sectoroverschrijdende, knelpunten die zijn gesignaleerd in literatuur en rechtspraak.

In hoofdstuk 5 wordt de knelpuntenanalyse gedaan meer specifiek gericht op de particuliere of private sector. Ook hier wordt vanuit de zes onderscheiden thema's geïnventariseerd welke de belangrijkste en meest in het oogspringende knelpunten er in de literatuur en rechtspraak zijn gesignaleerd, voorzover het gaat om deze sector.

In hoofdstuk 6 wordt dan de tweede van de sectorgerichte knelpuntenanalyses uitgevoerd. Dit betreft het de publieke sector. Ook hier wordt geïnventariseerd welke belangrijke knelpunten er in de literatuur en rechtspraak zijn gesignaleerd, voorzover het gaat om de toepassing van de Wbp.

In hoofdstuk 7 wordt de derde en laatste sectorgerichte knelpuntenanalyse uitgevoerd. Dit betreft de semi-publieke sector. Ook hier wordt geïnventariseerd welke knelpunten er in de literatuur en rechtspraak zijn gesignaleerd, voorzover het gaat om de toepassing van de Wbp in deze sector.

In hoofdstuk 8 worden ten slotte de bevindingen en resultaten van het onderzoek gepresenteerd vanuit het perspectief van de drie invalshoeken. Op basis daarvan worden aanbevelingen en suggesties gedaan voor de opzet en invulling van het tweede fase evaluatieonderzoek.

Een korte toelichting op de Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens of Wbp is op 1 september 2001 inwerking getreden en vervangt de Wet persoonsregistraties of WPR. De Wbp implementeert de richtlijn bescherming persoonsgegevens 95/46/EG die ook wel wordt aangeduid als de privacyrichtlijn.

De Wbp stelt regels voor het verwerken van 'persoonsgegevens', ofwel gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. De wet is van toepassing op geautomatiseerde verwerkingen van deze gegevens, en ook op de niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen, zoals een kaartenbak met adresgegevens of ander gestructureerde gegevensverzamelingen. De Wbp is echter niet van toepassing op het gebruik van persoonsgegevens uitsluitend voor persoonlijke of huishoudelijke doeleinden. Ook is de wet niet van toepassing op verwerkingen van persoonsgegevens door inlichtingen- en veiligheidsdiensten, verwerkingen door politie en justitie in het kader van de uitvoering van de politietaak.

De wet richt zich vooral tot de 'verantwoordelijke' – dat is de natuurlijke of rechtspersoon die zeggenschap heeft over de doeleinden waarvoor de gegevens worden verwerkt en de wijze waarop dat gebeurt. De natuurlijke personen over wie gegevens worden verwerkt worden aangeduid als de 'betrokkenen'. De Wbp verlangt dat persoonsgegevens op een behoorlijke en zorgvuldige manier worden verwerkt. Voordat een verantwoordelijke de gegevens mag verzamelen moet hij eerst bepalen voor welk doel of doelen hij dat doet. Daarnaast mag een verantwoordelijke alleen op basis van één of meer in de Wbp genoemde grondslagen persoonsgegevens verwerken. Voorbeelden van een grondslag zijn: ondubbelzinnige toestemming van de betrokkene; het uitvoeren van een overeenkomst met de betrokkene; het nakomen van een wettelijke verplichting; of een gerechtvaardigd (bedrijfs)belang. Voor bepaalde categorieën van persoonsgegevens, zoals gegevens over godsdienst, ras, gezondheid en strafrechtelijk verleden, gelden nog andere beperkingen. Dergelijke gegevens mogen in beginsel niet worden verwerkt, tenzij door bepaalde verantwoordelijken voor bepaalde doeleinden. Gezondheidsgegevens mogen bijvoorbeeld niet zonder meer door een willekeurige verantwoordelijke worden verwerkt, maar uiteraard wel door een huisarts in het kader van de behandeling van een patiënt.

De wet legt aan de verantwoordelijke een aantal informatieplichten op en verplichting om gegevensverwerkingen te melden bij het College bescherming persoonsgegevens (Cbp), tenzij de betreffende verwerking zijn vrijgesteld in het zgn Vrijstellingsbesluit. Voorbeelden van vrijgestelde verwerkingen zijn abonnementadministraties en salarisadministraties. Daarnaast kent de wet de betrokkenen een aantal rechten toe, zoals een inzage- of kennisnemingsrecht, een verbeterings- en een verwijderingsrecht en een verzetsrecht dat geldt in een aantal specifieke situaties.

De Wbp kent verder veel betekenis toe aan zelfregulering. Zo voorziet de wet in gedragscodes, waarin op sector- of brancheniveau nadere regels worden gesteld. Ook kent de wet de functionaris voor de gegevensbescherming (FG), een interne toezichthouder die zich binnen de organisatie van een verantwoordelijke bezig houdt met toezicht op en naleving van de wet.

Enkele onderdelen van de Wbp zijn uitgewerkt in AMvB's en ministeriele regelingen. De belangrijkste daarvan zijn het zo-even genoemde Vrijstellingsbesluit, waarin staat welk verwerkingen niet behoeven te worden gemeld, het Meldingsbesluit, dat vastlegt de meldingsformulieren vastleg, en het Besluit kostenvergoeding, dat aangeeft welke vergoeding de verantwoordelijke aan betrokkenen in rekening mag brengen als gebruik wordt gemaakt van het kennisnemings- of verzetsrecht.

Een praktisch uitleg van de wet geeft de door het Ministerie van Justitie uitgegeven Handleiding voor verwerkers van persoonsgegevens. Deze kan worden gedownload van de website van het Cbp, www.cbpweb.nl.

Hoofdstuk 2: Doelstellingen van de privacy-richtlijn

2.1 Inleiding

Dit onderdeel van deze studie betreft het eerste deel van de doelstellingeninventarisatie. Er wordt in kaart gebracht welke bedoelingen de gemeenschapswetgever heeft gehad met de privacy-richtlijn 95/46/EG, die de nationale wetgever heeft geïmplementeerd met de Wbp.

Deze implementatie is niet vrijblijvend.[9] Zoals alle richtlijnen is de privacy-richtlijn op grond van artikel 249 EG-Verdrag verbindend ten aanzien van het daarmee te bereiken resultaat. Dit betekent dat de nationale wetgever in verband met de verwerking van persoonsgegevens moet voorzien in waarborgen overeenkomstig de bepalingen van de richtlijn.[10] En hoewel de richtlijn niet uitgaat van volledige harmonisatie en voorziet in 'een zekere bandbreedte' bij de implementatie, is de nationale wetgever wel gehouden te voorzien in de door de richtlijn gestelde waarborgen. In zoverre moeten de doelstellingen van de richtlijn worden gezien als doelstellingen van de wet.

De belangrijkste bronnen voor dit onderdeel van de literatuurstudie zijn de privacy-richtlijn en de daarover gepubliceerde studies en rapporten, zoals het eerste Implementatierapport van de Europese Commissie over de implementatie van de richtlijn (het Implementatierapport),[11] alsmede enige rechtspraak van het Europees Hof van Justitie over de richtlijn. In aanvulling daarop is ook gebruik gemaakt van andere literatuur over de richtlijn.

2.2 Realiseren interne markt en bescherming fundamentele rechten

De privacy-richtlijn beoogt allereerst een bijdrage te leveren aan de algemene doelstellingen van de Gemeenschap. Deze liggen in het bevorderen van de betrekkingen tussen lidstaten en volkeren in de gemeenschap, het verzekeren van de economische en sociale vooruitgang, het verbeteren van de levensomstandigheden en het waarborgen en bevorderen van vrede en vrijheid en democratie, uitgaande van de fundamentele rechten.[12] Een en ander wordt wel samengevat als de Europese integratiegedachte.

De directe aanleiding voor de richtlijn waren de problemen[13] die zich in de jaren zeventig en tachtig voordeden met betrekking tot de toen in enkele lidstaten geldende nationale privacywetgeving. In deze wetgeving werden voorwaarden gesteld aan vastlegging en het gebruik van persoonsgegevens. Deze voorwaarden bleken betrekkelijk eenvoudig te kunnen worden omzeild door de gegevens via telecommunicatienetwerken over te brengen naar landen waar dergelijke wetgeving niet was. Om dit te voorkomen verbonden de lidstaten die wél beschikten over privacywetgeving in enkele gevallen strenge voorwaarden aan dergelijke gegevensoverdrachten – als ze deze overdrachten al niet geheel verboden.[14] En daarmee stond deze nationale privacywetgeving in de weg aan de integratiegedachte, en meer in het bijzonder aan de totstandbrenging en werking van wat in het Verdrag tot oprichting van de Europese Gemeenschap (EG-Verdrag) wordt aangeduid als een ruimte zonder binnengrenzen waarin het vrije verkeer van goederen, personen, diensten en kapitaal is gewaarborgd. Ofwel: de interne markt.[15]

---

[9] Zie over de implementatie van richtlijnen Cuijpers 2004, p. 82-83.
[10] Art. 1, eerste lid, richtlijn.
[11] First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003)265 final, Brussel, augustus 2003.
[12] Vgl. Art. 2 EG-Verdrag en art. 2 EU-Verdrag, alsmede overw. 1 en 2 richtlijn.
[13] Zie Van der Klaauw-Koops & Prins 2002, p.497; *Kamerstukken II* 1992-1993, 22 800 VI, nr. 43.
[14] Kuitenbrouwer 2002, p. 37.
[15] Vgl. *Kamerstukken II* 1992-1993, 22 800 VI, nr. 43; *Kamerstukken II* 1993-1994, 23 900 VI, nr. 13.

Om dit probleem op te lossen, zonder afbreuk te doen aan de in de mensenrechtenverdragen vastgelegde rechten op bescherming van een persoonlijke levenssfeer, deed de Commissie begin jaren negentig voorstellen voor een algemene privacy-richtlijn, die uiteindelijk hebben geleid tot de richtlijn van 24 oktober 1995 (95/46/EG). In deze privacy-richtlijn worden twee belangrijke ambities van de integratiegedachte belichaamd: enerzijds het realiseren van een interne markt en in dat kader het mogelijk maken van het vrije verkeer van persoonsgegevens, en anderzijds de bescherming van de fundamentele rechten en vrijheden van individuen. In de preambule van de richtlijn wordt met zoveel woorden aangegeven dat aan beide belangen evenveel betekenis toekomt:

> '...voor de totstandbrenging en de werking van de interne markt [...] niet alleen verkeer van persoonsgegevens van de ene lidstaat naar de andere mogelijk moet zijn, maar dat ook de fundamentele rechten van personen moeten worden beschermd.'[16]

De juridische grondslag van de richtlijn ligt evenwel in artikel 100A EG-Verdrag, thans vernummerd naar 95 EG-Verdrag.[17] Deze bepaling ziet op de harmonisering van nationale wetgeving ten behoeve van de totstandbrenging en werking van de interne markt. Om deze reden wordt er dan ook wel vanuit gegaan dat de richtlijn primair beoogt de belemmeringen weg te nemen die in de weg staan aan de interne markt. In het implementatierapport tekent de Commissie daarbij wel aan dat met de aanvaarding van het Handvest van de Grondrechten van de Europese Unie[18] in 2000 meer belang moet worden toegekend aan de bescherming van fundamentele rechten en vrijheden.[19] Ook kan worden gewezen op de rechtspraak van het Europees Hof van Justitie, met name het zgn. Österreichischer Rundfunk-arrest, waarin is uitgemaakt dat de richtlijn 95/46 moet worden uitgelegd op basis van de grondrechten die volgens vaste rechtspraak integrerend deel uitmaken van de algemene rechtsbeginselen welker eerbiediging het Hof verzekert.[20].

Zonder verder in te gaan op de rangorde of het relatieve gewicht van de beide door de richtlijn te dienen belangen kan worden vastgesteld dat de richtlijn een tweeledige hoofddoelstelling heeft met zowel een interne marktdimensie als een fundamentele rechtendimensie: de richtlijn beoogt enerzijds een bijdrage te leveren aan de totstandbrenging en werking van de interne markt en anderzijds waarborgen te bieden voor de bescherming van fundamentele rechten en vrijheden, in het bijzonder het recht op bescherming van een persoonlijke levenssfeer. [21]

---

[16] Vgl. ook overw. 1, 2, 10 en 11 richtlijn.

[17] Een verklaring of in elk geval een voordeel van de keuze voor artikel 100A of 95 EG-Verdrag als rechtsgrondslag is dat voor de aanvaarding van de daarop gebaseerde richtlijn op grond van artikel 251 EG-Verdrag slechts een gekwalificeerde meerderheid was vereist. Anders was eenparigheid van stemmen vereist. En omdat de richtlijn niet onomstreden was, wordt wel aangenomen dat meer dan zo een gekwalificeerde meerderheid indertijd niet haalbaar was. Zie daarover o.a. *Kamerstukken II* 1994-1995, 23 900 VI.

[18] Handvest van de Grondrechten van de Europese Unie, *PbEG* 2000, C364, 1-22.

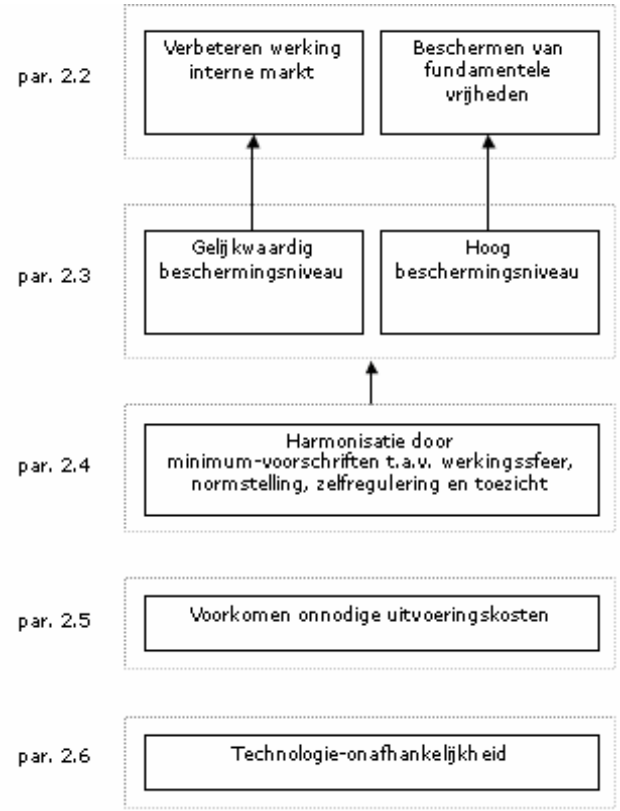
[19] Implementatierapport, p. 3-4; zie ook Economic Evaluation of the Data Protection Directive, p. 16 en 40-41.

[20] EHvJ 20 mei 2003 (Österreichischer Rundfunk), C-465/00, m.n. r.o. 68; zie ook EHvJ 6 maart 2001 (Connolly/Commissie), C-274/99P, r.o. 37. In haar annotatie bij het Österreichischer Rundfunk-arrest wijst Overkleeft-Verburg erop dat de uitspraak voor de toepassing van de richtlijn in concreto betekent dat eerst moet worden nagegaan of er sprake is van een inmenging in de persoonlijke levenssfeer en zo ja, of deze gerechtvaardigd is op grond van artikel 8 EVRM. Aldus G. Overkleeft-Verburg in *JB* 2004/112.

[21] Cuijpers 2004, p. 39-49; vgl. ook r.o. 41 van EHvJ 20 mei 2003 Zaken C-465/00, C-138/01 en C-139/01 (Österreichischer Rundfunk), waarin het Hof aangeeft dat 'voor een beroep op artikel 100A van het Verdrag als rechtsgrondslag niet [is] vereist, dat in elke situatie die valt onder een op deze grondslag gebaseerde handeling een daadwerkelijk verband met het vrije verkeer tussen lidstaten bestaat. [..] [A]rtikel 100 A van het Verdrag [kan] als rechtsgrondslag worden gebruikt wanneer de op die grondslag vastgestelde handeling daadwerkelijk tot doel heeft de voorwaarden voor de instelling en de werking van de interne markt te verbeteren'. Idem: r.o. 40 EHvJ 6 november 2003 Zaak C-101/01 (Lindqvist).

De richtlijn beoogt enerzijds een bijdrage te leveren aan de totstandbrenging en werking van de interne markt en anderzijds waarborgen te bieden voor de bescherming van fundamentele rechten en vrijheden, in het bijzonder het recht op bescherming van een persoonlijke levenssfeer.

In aanvulling op, of ter uitwerking van, deze tweeledige hoofddoelstelling kunnen er in de privacy-richtlijn nog een aantal andere doelstellingen worden onderscheiden. Een daarvan betreft de doelstelling van een gelijkwaardig beschermingsniveau, die een uitwerking betreft van de interne marktdimensie. Een andere betreft de doelstelling van een hoog beschermingsniveau, welke kan worden gezien als uitwerking van de fundamentele rechtendimensie. Daarnaast zijn er doelstellingen die zowel verband houden met de interne marktdimensie als de fundamentele rechtendimensie. Zo is harmonisatie het instrument om te komen tot het beoogde gelijkwaardige én hoge beschermingsniveau. Maar tegelijkertijd is harmonisatie een op zichzelf staande doelstelling, in zoverre dat de richtlijn, om te komen tot het gewenste gelijkwaardige en hoge beschermingsniveau, beoogt nationale wetgeving op elkaar af te stemmen.



Daarvan zijn weer te onderscheiden de doelstellingen die zien op bepaalde randvoorwaarden of kwaliteitsaspecten van de tot stand te brengen geharmoniseerde nationale wetgeving. Het gaat dan om de doelstelling om de uitvoeringskosten zo beperkt mogelijk te houden en de doelstelling van niet gemakkelijk te omzeilen en toekomstbestendige, dus technologie-onafhankelijke wetgeving. Een overzicht van de onderscheiden doelstellingen is op de volgende bladzijde van opgenomen. Deze doelstellingen worden in de volgende paragrafen van dit hoofdstuk nader uiteengezet.

2.3 Beschermingsniveau

De richtlijn beoogt te komen tot een gelijkwaardig en een hoog beschermingsniveau. De eerste doelstelling (het gelijkwaardige beschermingsniveau) is een direct uitvloeisel van de interne marktdimensie van de richtlijn. De tweede (het hoge beschermingsniveau) komt voort uit de fundamentele rechtendimensie.

2.3.1 Gelijkwaardig beschermingsniveau

Een uitwerking van de interne marktdimensie betreft het realiseren van een gelijkwaardig beschermingsniveau door het harmoniseren van de desbetreffende wet- en regelgeving van de lidstaten. Een gelijkwaardig beschermingsniveau betekent dat er geen sprake is van lidstaten met meer of minder bescherming, zodat er evenmin sprake van kan zijn dat binnen de gemeenschap de werking van de wetgeving wordt omzeild door gegevens te verwerken in een lidstaat met een lager beschermingsniveau. Er is dan dus voor lidstaten

geen aanleiding meer om vanwege de bescherming van de gegevens binnen de Unie belemmeringen voor het gegevensverkeer tussen lidstaten in stand te houden.[22]

In de preambule van de richtlijn wordt daarbij wel aangetekend dat niettemin aan de lidstaten een zekere vrijheid wordt gelaten die binnen het kader van de tenuitvoerlegging van de richtlijn kan worden gebruikt om de geboden bescherming te verbeteren. In dat verband wordt ook onderkend dat dit aanleiding kan zijn voor ongelijkheden bij de tenuitvoerlegging van de richtlijn, die gevolgen kunnen hebben voor het gegevensverkeer binnen een lidstaat en de Unie.

De richtlijn beoogt binnen een zekere bandbreedte door harmonisering van wetgeving te komen tot een gelijkwaardig beschermingsniveau voor alle lidstaten.

2.3.2 Hoog beschermingsniveau

Een uitwerking van de fundamentele rechtendimensie van de primaire doelstelling betreft het verbeteren van de door de wetgeving geboden bescherming en het streven naar een hoog beschermingsniveau.[23] Het door harmonisatie te bereiken gelijkwaardige beschermingniveau mag, aldus blijkt uitdrukkelijk uit de preambule van de richtlijn, niet leiden tot een verzwakking van de aldus geboden bescherming, maar moet juist zijn gericht op een hoog beschermingsniveau. En van de nationale wetgever wordt daarbij verwacht dat hij ernaar streeft om de indertijd geboden bescherming te verbeteren.[24]

In dat verband verwijst de richtlijn naar het Europees Verdrag tot bescherming van de Rechten van de Mens (EVRM)[25] en naar het op artikel 8 daarvan gebaseerde Verdrag tot bescherming van personen terzake van de geautomatiseerde verwerking van persoonsgegevens (Verdrag inzake gegevensbescherming), dat door de lidstaten is ondertekend en geratificeerd.[26] De richtlijn beoogt de beginselen van dit verdrag te verduidelijken en te versterken.[27]

De richtlijn is gericht op een hoog beschermingsniveau en beoogt de privacybeginselen van het Verdrag inzake gegevensbescherming te verduidelijken en te versterken.

2.4 Harmonisatie

De richtlijn strekt ertoe het beoogde gelijkwaardige en hoge beschermingsniveau te realiseren door nationale privacywetten[28] op elkaar afstemmen. Harmonisatie is derhalve het instrument om het gewenste beschermingsniveau te bereiken. Tegelijkertijd kan deze harmonisatie worden gezien als een op zichzelf staande doelstelling van de richtlijn: de richtlijn beoogt nationale wetgeving te harmoniseren en doet dat door minimumvoorschriften te geven waaraan deze nationale wetgeving moet voldoen. Over deze har-

---

[22] Overw. 7 t/m 9 richtlijn.
[23] Overw. 9 richtlijn.
[24] Overw. 9 richtlijn.
[25] Overw. 10 richtlijn.
[26] Zie voor een uiteenzeting van de verhouding tussen de richtlijn en het Verdrag inzake gegevensbescherming: Van der Klaauw-Koops & Prins 2002, p. 499.
[27] Overw. 11 richtlijn.
[28] In dit rapport wordt de term 'privacywet' in aansluiting op het ingeburgerde (maar misschien niet helemaal correcte) taalgebruik ook gebruikt als aanduiding van de wetgeving gericht op de bescherming van persoonsgegevens. Zie voor de discussie over de verhouding tussen 'privacy' en 'gegevensbescherming' of 'data protectie' bijvoorbeeld Blok 2002, Berkvens 2004b, p. 267 of Holvast & Prins 2003, p. 66.

monisatie-doelstelling wordt in de preambule van de richtlijn met verwijzing naar het subsidiariteitsbeginsel overwogen:

> 'dat dit doel [van een gelijkwaardig en hoog beschermingsniveau], dat voor de interne markt van fundamenteel belang is, niet kan worden bereikt door een optreden van de Lid-Staten alleen, gezien met name de omvang van de bestaande divergenties tussen de geldende nationale wettelijke regelingen ter zake en de noodzaak om de wetgevingen van de Lid-Staten op elkaar af te stemmen teneinde voor de grensoverschrijdende stromen van persoonsgegevens tot een samenhangende reglementering te komen die in overeenstemming is met de doelstelling van de interne markt.'

De door de richtlijn beoogde harmonisatie is niet volledig. Op verschillende deelterreinen biedt de richtlijn de nationale wetgever 'een zekere vrijheid' of 'bandbreedte' om de wetgeving naar eigen inzichten in te richten. Met daarbij de aantekening dat er wel moet worden gestreefd naar het verbeteren van de geboden bescherming. De harmonisatiedoelstelling van de richtlijn kan dan worden samengevat als het streven om de relevante nationale privacywetten van lidstaten met elkaar in overeenstemming te brengen en ervoor zorg te dragen dat er in de verschillende lidstaten soortgelijke aanspraken en verplichtingen gelden ten aanzien van de bescherming van persoonsgegevens.

De richtlijn beoogt nationale privacywetten van lidstaten met elkaar in overeenstemming brengen en ervoor zorg te dragen dat in de verschillende lidstaten soortgelijke aanspraken en verplichtingen gelden ten aanzien van de bescherming van persoonsgegevens.

Om te komen tot geharmoniseerde nationale wetgeving bevat de richtlijn minimumvoorschriften waaraan de wetgeving van de lidstaten moet voldoen. Ook ten aanzien van deze voorschriften heeft de gemeenschapswetgever keuzes gemaakt waaraan weer allerlei bedoelingen ten grondslag liggen. Deze keuzes heeft de gemeenschapswetgever uiteraard gemaakt binnen de kaders van het gemeenschapsrecht. Dat laatste betekent dat de richtlijn geen betrekking heeft op de activiteiten die niet onder de toepassing van het gemeenschapsrecht vallen, te weten de in titels V en VI van het Verdrag van de Europese Unie bedoelde activiteiten met betrekking tot openbare veiligheid, defensie, staatsveiligheid en de activiteiten van de Staat op strafrechtelijk gebied.[29] En daarnaast komt natuurlijk betekenis toe aan het subsidiariteitsbeginsel, dat voorschrijft dat de gemeenschapswetgever alleen mag optreden voorzover de met dat optreden te bereiken doelen niet voldoende kunnen worden bereikt door optreden van de lidstaten.[30]

De in de richtlijn gestelde voorschiften hebben betrekking op de onderwerpen die, gelet op de met de harmonisatie beoogde doelen, door alle lidstaten in elk geval op dezelfde wijze moeten worden geregeld. Deze onderwerpen zijn achtereenvolgens:

- werkingssfeer en toepassing;
- normatieve kaders;
- zelfregulering;
- transparantie en rechten van betrokkenen;
- toezicht en rechtsbescherming;
- internationale gegevensdoorgifte.

In het navolgende wordt ingegaan op de bij deze onderwerpen gemaakte keuzes en de bedoelingen die de gemeenschapswetgever daarbij blijkens de richtlijn en de preambule daarbij heeft.

---

[29] Overw. 13 en 16, alsmede art. 3, tweede lid, richtlijn.
[30] Art. 5 EG-Verdrag.

2.4.1 Werkingsfeer en toepassing

De richtlijn heeft betrekking op de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en op het vrije verkeer van die gegevens. De richtlijn gaat over grensoverschrijdend gegevensverkeer en het harmoniseren van nationale wetgeving teneinde de belemmeringen weg te nemen die in de weg staan aan de totstandbrenging en werking van de interne markt.[31] Waar het gaat om de werkingssfeer, toepassing en reikwijdte van de richtlijn kunnen de door de gemeenschapswetgever gemaakte keuzes vooral worden verklaard vanuit de interne marktdimensie. Anders gezegd, voor de werkingssfeer is vooral bepalend dat de richtlijn beoogt de interne markt-belemmeringen weg te nemen, hoewel er ook wel wat redenen zijn die mede voortkomen uit de fundamentele rechtendimensie van de richtlijn.

Alle verwerkingen die onder het gemeenschapsrecht vallen

Voor de werkingssfeer en reikwijdte is allereerst van belang dat de richtlijn uitgaat van nadrukkelijk zeer algemeen gedefinieerde en veelomvattende begrippen 'persoonsgegeven' en 'verwerking'.[32] Uitgaande van deze begrippen stelt de gemeenschapswetgever voorop dat de door de richtlijn te bieden bescherming zich uitstrekt over alle persoonsgegevensverwerkingen die vallen onder de werkingssfeer van het gemeenschapsrecht. Al deze gegevensverwerkingen moeten worden uigevoerd overeenkomstig de wetgeving van een van de lidstaten – dit om te voorkomen dat een persoon wordt uitgesloten van de bescherming waarop hij krachtens de richtlijn recht heeft.[33]

Alleen geautomatiseerde verwerkingen en gegevens in bestanden

Op het uitgangspunt dat de richtlijn geldt ten aanzien van alle verwerkingen worden wel enkele beperkingen aangebracht. Zo is de werkingssfeer van de richtlijn beperkt tot geheel of gedeeltelijk geautomatiseerde verwerkingen en niet-geautomatiseerde verwerkingen alleen voorzover deze betrekking hebben op bestanden, te weten: verzamelingen van persoonsgegevens die volgens specifieke persoonscriteria zijn gestructureerd teneinde gemakkelijke toegang tot de gegevens mogelijk te maken.[34]

De reden waarom de richtlijn van toepassing is op geautomatiseerde verwerkingen wordt niet met zoveel woorden uiteengezet in de tekst van de richtlijn en de preambule daarvan. Aangenomen kan worden dat dit verband houdt met de omstandigheid dat vooral dergelijke verwerkingen via telecommunicatienetwerken betrekkelijk eenvoudig kunnen worden overgebracht naar landen met een lager beschermingsniveau. Er is bij deze geautomatiseerde verwerkingen daardoor een groter risico op privacyinbreuken en dus ook op interne markt-belemmeringen die het gevolg kunnen zijn van wettelijke bescherming tegen dergelijke inbreuken.[35]

Waarom de gemeenschapswetgever de niet-geautomatiseerde gegevensverwerkingen van gegevens in gestructureerde gegevensverzamelingen ook onder de werkingssfeer van de richtlijn heeft gebracht is minder vanzelfsprekend. Vanwege de toegankelijkheid van deze gestructureerde gegevensverzamelingen is er bij deze verwerkingen misschien een vergroot risico van privacyinbreuken. Maar omdat het gaat om niet-geautomatiseerde verwerkingen moet toch ook worden aangenomen dat er in veel minder mate sprake kan

---

[31] Vgl. overw. 7 en 8 richtlijn.
[32] Art. 2, onder a en b, richtlijn; in overw. 14 richtlijn wordt enigszins ten overvloed aangegeven dat de richtlijn, gelet op de ontwikkeling van informatietechnieken, ook van toepassing is op beeld- en geluidsgegevens. En hoewel dat niet met zoveel woorden wordt gezegd zal wel bedoeld zijn dat beelden en geluiden ook persoonsgegevens kunnen zijn. Vgl. ook overw. 26 waarin staat dat om te bepalen of een persoon identificeerbaar is moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat deze redelijkerwijs in te zetten zijn om de genoemde persoon te identificeren.
[33] Overw. 12 richtlijn.
[34] Art. 3, eerste lid, en overw. 15 richtlijn.
[35] Vgl. ook overw. 6 richtlijn.

zijn van grensoverschrijdend gegevensverkeer, waardoor belemmeringen van de interne markt niet heel erg aannemelijk zijn. De reden om toch ook niet deze niet-geautomatiseerde verwerkingen onder de werkingssfeer van de richtlijn te brengen moet dan ook worden gezocht in de wens van enkele lidstaten, waaronder Nederland, dat de richtlijn geen afbreuk zou doen aan de bescherming van de persoonlijke levenssfeer zoals deze was geregeld in reeds geldende nationale privacywetgeving.[36]

In de preambule van de richtlijn wordt opgemerkt dat lidstaten zelf de criteria mogen vaststellen op basis waarvan wordt bepaald of een niet-geautomatiseerde verwerking onder de werkingssfeer valt of niet.[37] De lidstaten hebben daarmee dus de mogelijkheid de omvang van de niet-geautomatiseerde verwerkingen die onder de werkingssfeer valt te beperken tot die waarvoor zij dat, mede gelet op de doelstellingen van de richtlijn, nodig achten.

Geen verwerkingen met uitsluitend persoonlijke of huishoudelijke doeleinden

Een andere beperking van de werkingssfeer van de richtlijn betreft de gegevensverwerkingen die door natuurlijke personen worden verricht in het kader van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden, zoals correspondentie en het bijhouden van adresbestanden.[38] Dit betreft verwerkingen waarvan de gemeenschapswetgever aannam dat deze geringe risico's op privacyinbreuken met zich mee brengen en als zodanig weinig aanleiding geven voor belemmeringen van de interne markt. Als het gaat om verwerkingen voor persoonlijke of huishoudelijke doeleinden ligt grensoverschrijdend gegevensverkeer minder voor de hand. Althans, als wordt uitgegaan van technologische context ten tijde van de totstandkoming van de richtlijn.[39]

Om de interne marktbelemmeringen weg te nemen heeft de richtlijn een ruime werkingssfeer die vooral ziet op geautomatiseerde verwerkingen en niet de verwerkingen voor huishoudelijke en persoonlijke doeleinden. In hoeverre de werkingssfeer ook niet-geautomatiseerde verwerkingen omvat wordt overgelaten aan de nationale wetgever.

Territoriale toepassing

Het kunnen bepalen welke wet van toepassing is op gegevensverwerkingen is vooral van belang waar het gaat om verwerkingen met een lidstaatoverschrijdend karakter of om verwerkingen die worden uitgevoerd door of vanwege een verantwoordelijke die zich in meerdere lidstaten bevindt. De gemeenschapswetgever heeft ervoor gekozen uit te gaan van de vestigingsplaats of vestigingsplaatsen van de verantwoordelijke, waarbij de rechtsvorm van de vestiging[40] als zodanig niet doorslaggevend is. Van toepassing is de privacywet van het land waar de desbetreffende vestiging zich bevindt, als er gegevens worden verwerkt in het kader van activiteiten van die vestigingen.[41] Dit betekent dat een verantwoordelijke met vestigingen in meerdere lidstaten te maken kan hebben met verschillende nationale privacywetten die van toepassing zijn op de verwerkingen van de verschillende vestigingen.[42]

Daarbij bepaalt de richtlijn dat de nationale privacywetgeving van toepassing is op verwerkingen die worden verricht door verantwoordelijken van buiten de EU die gebruik maken van al dan niet geautomati-

---

[36] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 5.
[37] Overw. 27 richtlijn.
[38] Art. 3, tweede lid, eerste gedachtenstreepje, en overw. 12 richtlijn.
[39] Vgl. EHvJ 6 november 2003, zaak C101/01, *PbEG* 2003, p. I-12971, waarin het Hof met zoveel woorden zegt dat de gemeenschapswetgever de ontwikkeling van internet niet had voorzien.
[40] Het begrip vestiging is o.a. ingevuld in de rechtspraak van het Europees Hof van Justitie, zie: EHvJ4 december 1986, zaak 205/84, *PbEG* 1986, p. 3755, r.o. 21 en EHvJ 10 mei 1995, zaak C-384/93, *NJ* 1995, 703.
[41] Art. 4, eerste lid, richtlijn.
[42] Prins & Berkvens 2002, p. 100.

seerde middelen (zoals een server of backup faciliteiten) op het grondgebied van een lidstaat. In dat geval is de wetgeving van de desbetreffende lidstaat van toepassing, tenzij deze al dan niet geautomatiseerde middelen alleen voor de doorvoer van gegevens worden gebruikt.[43]

Uit de richtlijn zelf blijkt dat de gemeenschapswetgever met deze toepasselijkheidsregels beoogt te voorkomen dat betrokkenen worden uitgesloten van de bescherming waarop zij krachtens de richtlijn aanspraak maken, alsmede om te voorkomen dat de wetgeving wordt ontdoken.[44] Het is niet duidelijk waarom er niet is gekozen voor bijvoorbeeld een country-of-origin-regel,[45] die multinationals de gelegenheid zou bieden om te kiezen voor een toepasselijke nationale wet.[46] Een reden zou kunnen zijn gelegen in de omstandigheid dat de richtlijn op onderdelen ruimte laat voor een eigen invulling door nationale wetgevers, welke door zo een country-of-origin-regel zouden kunnen worden omzeild.

Om ontduiking van nationale wetgeving te voorkomen is nationale wetgeving die de richtlijn implementeert van toepassing op de verwerkingen die worden verricht in het kader van activiteiten van een vestiging van de verantwoordelijke, alsmede op de verwerkingen die plaatsvinden met behulp van middelen op het grondgebied van een lidstaat, tenzij die alleen voor de gegevensdoorvoer worden gebruikt. Voor de vraag welke nationale wet van toepassing is gaat het dus om de plaats waar de verantwoordelijke is gevestigd, dan wel, als deze niet in de EU is gevestigd, om de plaats waar de gegevens worden verwerkt.

2.4.2 Normatieve kaders

Waar het gaat om de normatieve kaders is duidelijk dat de voorschriften in de richtlijn nodig zijn voor het totstandbrenging van zowel het hoge als het gelijkwaardige beschermingsniveau. De richtlijn geeft deze voorschriften om te komen tot de beoogde geharmoniseerde wetgeving, die is gericht op het waarborgen van een hoog beschermingsniveau en die in elk geval niet minder bescherming biedt dan artikel 8 EVRM en het Verdrag inzake gegevensbescherming. Ook wil de richtlijn met deze voorschriften de beginselen van dat verdrag verduidelijken en versterken.[47]

De richtlijn geeft de belangrijkste aan gegevensverwerkingen te stellen voorwaarden. Het gaat dan onder meer om de verwerkingsgrondslagen, doelbinding- en beveiligingsvereisten, meldingverplichtingen, vereisten met betrekking tot de doorgifte van gegevens naar derde-landen enz.[48] De daarmee te bieden bescherming moet bestaan uit verplichtingen voor degenen die de gegevens verwerken en kennisnemings- en andere rechten voor de personen over wie gegevens worden verwerkt.[49] Verder geeft de richtlijn aan wanneer welke nationale privacywetgeving van toepassing is.[50] Op een aantal deelgebieden wordt de nationale wetgever ruimte gelaten om te kiezen voor een eigen invulling van de wetgeving. Voor gegevensverwerkingen in specifieke sectoren en voor specifieke categorieën van bijzondere of gevoelige gegevens kan de wetgever aanvullende eigen regels stellen.[51] En als de wetgever voorziet in passende waarborgen kan de wetgever ook zorgdragen voor minder strenge regels voor de gegevensverwerkingen voor historische, statistische of wetenschappelijke doeleinden. Ook staat de richtlijn toe dat de nationale wetgever voorziet in

[43] Art. 4, tweede lid, richtlijn.
[44] Overw. 18-20 richtlijn.
[45] D.w.z. een regel op basis waarvan de privacywet van het land van de hoofdvestiging van de verantwoordelijke van toepassing zou zijn op de verwerkingen die worden verricht al dan niet door door dochterondernemingen elders in de EU worden gedaan.
[46] Vgl. Implementatierapport p. 17.
[47] Overw. 10 e.v. richtlijn.
[48] Art. 5 t/m 21 en overw. 22, 28 t/m 36 richtlijn.
[49] Art. 10 t/m 12 en overw. 25, 38 t/m 46.
[50] Art. 4 en overw. 19 en 20 richtlijn.
[51] Overw. 22 richtlijn.

een regeling voor verwerkingen die door hun aard, reikwijdte of doel een bijzonder risico kunnen betekenen voor de rechten van de betrokkenen.[52]

De redenen om voor deze en andere verwerkingen de nationale wetgever enige ruimte te geven liggen in het mogelijk maken dat de wetgeving rekening kan houden met specifieke nationale omstandigheden, waarop de gemeenschapswetgever minder of geen zicht heeft. Deze redenen houden dus verband met het subsidiariteitsbeginsel: om zoveel mogelijk tegemoet te komen aan de bijzonderheden van bepaalde categorieën van gegevens of verwerkingen of risico's wordt het in de aangegeven gevallen beter geacht dat de nationale wetgever zijn eigen invulling kan geven aan de wetgeving.

De richtlijn beoogt waar mogelijk tegemoet te komen aan de bijzonderheden van bepaalde categorieën van gegevens of verwerkingen of risico's en biedt de nationale wetgever in aangegeven gevallen de mogelijkheid om een eigen invulling te geven aan de wetgeving.

2.4.3 Zelfregulering

In het verlengde van de in de voorgaande subparagraaf even omschreven doelstelling – harmonisatie met de ruimte om waar mogelijk een eigen invulling te geven – is het streven om door middel van zelfregulering mogelijk te maken dat zoveel mogelijk rekening wordt gehouden met de specifieke behoeften van bepaalde sectoren of beroepsgroepen. De richtlijn voorziet daartoe nadrukkelijk in een 'zeker vrijheid' waarvan bij de uitvoering van de richtlijn gebruik kan worden gemaakt door de sociale en economische partners.'[53] Artikel 27 van de richtlijn verlangt dan ook uitdrukkelijk dat wordt bevorderd dat op branche- en sectorniveau gedragscodes worden opgesteld waarmee rekening wordt gehouden met de specifieke omstandigheden en behoeften van de desbetreffende sector of branche. In de preambule wordt overwogen dat de richtlijn beoogt:

> '...de betrokken beroepsgroepen [...] aan te moedigen gedragscodes op te stellen om, rekening houdend met het specifieke karakter van de verwerkingen in sommige sectoren, de uitvoering van de richtlijn te bevorderen'.[54]

De richtlijn beoogt dat zoveel mogelijk rekening kan worden gehouden met de specifieke omstandigheden en behoeften van de sector of branche. Daartoe beoogt de richtlijn te bevorderen dat op branche- en sectorniveau gedragscodes worden opgesteld.

2.4.4 Transparantie en rechten van betrokkenen

Het vergroten van de transparantie van verwerkingen wordt vooral gezien als uitwerking van de fundamentele rechtendimensie. Maar daarnaast kan transparantie ook worden gezien in het licht van de interne marktdimensie, aangezien de kenbaarheid van gegevensverwerkingen bepalend is voor de mogelijkheden van betrokkenen en/of de toezichthouder om iets te kunnen doen tegen de niet-naleving van de richtlijn. In zoverre kan het verbeteren van de transparantie van gegevensverwerkingen dus ook worden gezien in termen van waarborgen tegen aantasting van het (in alle lidstaten) gelijkwaardige beschermingsniveau.

De richtlijn lijkt transparantie evenwel vooral te zien als middel om te komen tot een hoog beschermingsniveau. In artikel 21, eerste lid, verlangt de richtlijn dat lidstaten maatregelen nemen om te zorgen voor de openbaarheid van de verwerkingen. In de preambule wordt daarover overwogen:

---

[52] Art. 8 en overw. 53 richtlijn.
[53] Overw. 9 richtlijn.
[54] Overw. 61 richtlijn.

> 'dat eerlijke verwerking van gegevens veronderstelt dat de betrokkenen van het bestaan van de verwerkingen op de hoogte kunnen zijn en, wanneer van hen gegevens worden verkregen, daadwerkelijk en volledig worden ingelicht over de omstandigheden waaronder deze gegevens worden verkregen'.[55]

In dat verband wordt, uiteraard, betekenis toegekend aan de wijze waarop de gegevens worden verkregen. Waarborgen ten aanzien van de transparantie van verwerkingen zijn vooral nodig waar het gaat om gegevens die niet van de betrokkenen zelf worden verkregen. In de preambule wordt opgemerkt:

> 'dat bepaalde verwerkingen betrekking hebben op gegevens die de verantwoordelijke niet rechtstreeks van de betrokkene heeft verkregen; dat gegevens voorts rechtmatig kunnen worden meegedeeld aan een derde, ook al was zulks ten tijde van het verkrijgen van de gegevens van de betrokkene niet voorzien; dat in al deze gevallen de informatie aan de betrokkene dient te worden verstrekt op het moment van de registratie van de gegevens of, uiterlijk, wanneer de gegevens voor de eerste maal aan een derde worden meegedeeld'.[56]

Bij het verbeteren van de transparantie van gegevensverwerkingen is ook een rol weggelegd voor de toezichthoudende instantie. Deze moet, zo blijkt uit artikel 21, tweede lid, van de richtlijn een door iedereen te raadplegen register bijhouden waarin belangrijke gegevens over gemelde verwerkingen zijn opgenomen, zoals contactgegevens van de verantwoordelijke, verwerkingsdoeleinden, de betrokkenen en de verwerkte gegevens, ontvangers van de gegevens en de voorgenomen overdrachten van de gegevens naar derde landen. In de preambule wordt aangegeven wat daarvan de bedoeling is. Er wordt overwogen dat:

> '…de aanmelding bij de toezichthoudende autoriteit strekt tot de openbaarmaking van het doel van de gegevensverwerking en van de belangrijkste kenmerken ervan, opdat een en ander aan de ter uitvoering van deze richtlijn vastgestelde nationale bepalingen kan worden getoetst'.[57]

Om te komen tot een hoog beschermingsniveau beoogt de richtlijn de transparantie van gegevensverwerkingen te verbeteren door te voorzien in waarborgen voor betrokkenen. Deze bestaan uit verplichtingen voor verantwoordelijken en aanspraken voor betrokkenen.

2.4.5 Toezicht en rechtsbescherming

Als de tot stand te brengen geharmoniseerde nationale privacywetgeving niet wordt nageleefd of niet wordt gehandhaafd heeft dat uiteraard gevolgen voor het door de richtlijn beoogde gelijkwaardige en hoge beschermingsniveau. Als de nationale wetgeving niet wordt nageleefd wordt afbreuk gedaan aan het gelijkwaardige beschermingsniveau en daarmee aan de totstandbrenging van de interne markt. Tegelijkertijd gaat niet-naleving ten koste van het hoge beschermingsniveau. In zoverre kunnen de bepalingen met betrekking tot toezicht, handhaving en rechtsbescherming worden gezien vanuit zowel de interne marktdimensie als de fundamentele rechten dimensie. De richtlijn voorziet in een aantal waarborgen tegen nietnaleving, te weten via een onafhankelijke toezichthouder met uitgebreide bevoegdheden, door toegang tot de rechter te verzekeren en betrokkenen aanspraken te geven op schadevergoeding, en door te voorzien in passende sancties

[55] Overw. 38 richtlijn.
[56] Overw. 39 richtlijn.
[57] Overw. 48 richtlijn.

Toezicht

Voor de bescherming van personen in verband met de verwerking van persoonsgegevens vindt de gemeenschapswetgever het 'van wezenlijk belang' dat er een onafhankelijke toezichthouder wordt ingesteld.[58] Deze toezichthouder is belast met het toezicht op de toepassing en naleving van de privacywetgeving waarmee uitvoering is gegeven aan de richtlijn. En daartoe moet deze toezichthouder beschikken over de nodige middelen om zijn taken te kunnen uitoefenen, waaronder in elk geval onderzoeksbevoegdheden en bevoegdheden om zonodig actief te kunnen ingrijpen in en te kunnen optreden tegen verwerkingen in strijd met deze privacywetgeving. Ook moet de toezichthouder bijdragen aan de doorzichtigheid van de verwerking van gegevens. [59]

Toegang tot de rechter en schadevergoeding

Verder beoogt de richtlijn dat wordt voorzien in een minimum aan rechtsbescherming tegen niet eerbiediging van de door de richtlijn beoogde bescherming. Als daarvan sprake is moet, zo blijkt uit artikel 22 van de richtlijn, de betrokkene dit aan een rechter kunnen voorleggen. In voorkomende gevallen moet, aldus artikel 23 van de richtlijn, de betrokkene aanspraak kunnen maken op schadevergoeding door de verantwoordelijke. In artikel 22 bepaalt de richtlijn daartoe dat iedereen zich tot de rechter kan wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden.

Sancties

Verder verlangt de richtlijn in artikel 24 dat lidstaten passende maatregelen nemen om de onverkorte toepassing van de bepalingen van deze richtlijn te garanderen. Er moet daarvoor worden voorzien in sancties die gelden bij inbreuk op de ter uitvoering van deze richtlijn vastgestelde bepalingen.

De richtlijn beoogt naleving van de privacywet te verzekeren door te voorzien in een onafhankelijke toezichthouder en toegang tot de rechter en de mogelijkheid van schadevergoeding, alsmede door passende sancties.

2.4.6 Internationale gegevensdoorgifte

De gemeenschapswetgever heeft ingezien dat het internationale handelsverkeer niet ophoudt bij de gemeenschapsgrenzen en voorziet daarom in minimumvoorschriften voor de doorgifte van gegevens naar landen buiten de gemeenschap, de zgn. derde landen. De bedoeling van deze voorschriften ligt in het voorkomen dat het beoogde gelijkwaardige en hoge beschermingsniveau wordt omzeild of ontdoken.

De richtlijn staat toe dat persoonsgegevens worden doorgegeven naar derde landen die voorzien in een beschermingniveau dat, gelet op de richtlijn, als passend kan worden gezien. En daarbij verbiedt de richtlijn de doorgifte naar derde landen als deze niet zo een passend beschermingsniveau bieden, tenzij er is voldaan aan een aantal voorwaarden. De richtlijn beoogt daarmee het internationale handelsverkeer niet onnodig te belemmeren en tegelijkertijd geen afbreuk te doen aan het te realiseren gelijkwaardige en hoge beschermingsniveau.[60] De richtlijn beoogt, zoals de Artikel 29 Werkgroep het zegt, zorg te dragen:

> 'voor een goed evenwicht tussen de bescherming van personen van wie de gegevens zullen worden doorgegeven aan landen zonder passend beschermingsniveau, enerzijds, en

[58] Overw. 62 richtlijn.
[59] Overw. 63 richtlijn.
[60] Art. 25-26 en overw. 56-60 richtlijn.

"de gerechtvaardigde wensen van de internationale handel en de realiteit van wereldomspannende telecommunicatienetwerken", anderzijds.'[61]

De richtlijn beoogt het internationale handelsverkeer niet onnodig te belemmeren en tegelijkertijd geen afbreuk te doen aan het te realiseren gelijkwaardige en hoge beschermingsniveau

2.5 Uitvoeringskosten

Het streven om de uitvoeringskosten van de richtlijn te beperken wordt als zodanig nauwelijks in de richtlijn en de preambule daarvan genoemd. In het Implementatierapport gaat de Commissie wel kort in op het streven naar een vereenvoudiging van de regelgeving in het belang van zowel 'good governance' als 'competitiveness':

'The Commission takes a view of the overall policy objectives to be pursued by Internal Market legislation that goes beyond mere free movement. This should provide a level playing field for economic operators in different Member States; help to simplify the regulatory environment in the interests of both good governance and competitiveness; and tend to encourage rather than hinder cross-border activity within the EU'.[62]

Het gaat hier om een van de kwaliteitsaspecten van de te tot stand te brengen geharmoniseerde nationale wetgeving. In min-of-meer dezelfde lijn zijn enkele overwegingen in de richtlijn die zijn gericht op het beperken van de kosten voor verantwoordelijken die de wet moeten naleven. Het gaat dan met name om de meldplicht:

'Overwegende dat, om inadequate administratieve formaliteiten te vermijden, voor de verwerkingen die geen inbreuk kunnen maken op de rechten en vrijheden van de betrokkenen, in vrijstelling of vereenvoudiging van de aanmelding kan worden voorzien, mits deze verwerkingen in overeenstemming zijn met een door de Lid-Staat genomen besluit, waarin de grenzen van een en ander worden aangegeven; dat de Lid-Staten eveneens in vrijstelling of vereenvoudiging kunnen voorzien wanneer een persoon die door de voor de verwerking verantwoordelijke is aangewezen zich ervan vergewist dat de verwerkingen geen inbreuk op de rechten en vrijheden van de betrokkenen kunnen maken'. [63]

De richtlijn beoogt dus inadequate administratieve formaliteiten te vermijden. En hoewel de tekst van de richtlijn zich daarbij lijkt te beperken tot de kosten verband houdend met de meldplicht ligt het in de rede dat de gemeenschapswetgever dit ook in meer algemene zin beoogt.

De richtlijn beoogt met name waar het gaat om de meldplicht te voorkomen dat verantwoordelijken te maken hebben met onnodige uitvoeringskosten.

2.6 Technologie-onafhankelijkheid

Ook technologie-onafhankelijkheid ziet meer op de kwaliteitsaspecten van wetgeving dan op een hoog of gelijkwaardig beschermingsniveau. Daarmee is niet gezegd dat de mate van technologieafhankelijkheid niet van belang is voor respectievelijk de interne markt- of de fundamentele rechtendimensies: wetgeving die onvoldoende technologie-onafhankelijk is loopt het risico niet meer doeltreffend te zijn als er zich techno-

[61] Art. 29 Werkgroep 2005b, p. 2.
[62] Implementatierapport, p. 10-11.
[63] Overw. 49 richtlijn.

logische ontwikkelingen voordoen. En dat doet afbreuk aan zowel de hoogte als de gelijkwaardigheid van het beschermingsniveau.

Over technologie-onafhankelijkheid is in de preambule van de richtlijn alleen opgenomen dat de reikwijdte van de bescherming niet afhankelijk mag zijn van de gebruikte technieken, omdat dat een ernstig risico voor ontduiking zou opleveren. In de preambule wordt daartoe, waar het gaat om het onderscheid tussen geautomatiseerde en niet-geautomatiseerde verwerkingen overwogen dat:

> 'de bescherming van personen zowel op automatische als op niet-automatische verwerking van toepassing is; dat de reikwijdte van deze bescherming in feite niet afhankelijk mag zijn van de gebruikte technieken, omdat zulks ernstig gevaar voor ontduiking zou opleveren'.[64]

Verder wordt op enkele plaatsen in de preambule verwezen naar technologische en andere ontwikkelingen waardoor de verwerking van persoonsgegevens, daaronder mede begrepen geluid- en beeldgegevens, aanzienlijk wordt vergemakkelijkt. De richtlijn beoogt nadrukkelijk dat ook regels worden gesteld voor dergelijke verwerkingen.[65] Er kan op basis daravan worden aangenomen dat de richtlijn technologie-onafhankelijke wetgeving beoogt – en dat omdat zo wordt voorkomen dat de richtlijn bij technologische ontwikkelingen niet meer zou gelden of ontdoken kan worden doordat gebruik wordt gemaakt van de een technologie waarin de gemeenschapswetgever niet had voorzien.

De richtlijn beoogt technologie-onafhankelijke wetgeving, zodat bescherming gewaarborgd blijft als er zich technologische ontwikkelingen voordoen.

2.7 Conclusies

De richtlijn beoogt enerzijds een bijdrage te leveren aan de totstandbrenging en werking van de interne markt en anderzijds waarborgen te bieden voor de bescherming van fundamentele rechten en vrijheden, in het bijzonder het recht op bescherming van een persoonlijke levenssfeer. De richtlijn beoogt deze tweeledige doelstelling te verwezenlijken door via harmonisering van de nationale wetgeving te komen tot een gelijkwaardig beschermingsniveau voor alle lidstaten. Verder is de richtlijn gericht op een hoog beschermingsniveau en beoogt deze de privacybeginselen van het Verdrag inzake gegevensbescherming te verduidelijken en te versterken.

De richtlijn beoogt nationale privacywetten van lidstaten met elkaar in overeenstemming te brengen en ervoor zorg te dragen dat in de verschillende lidstaten soortgelijke aanspraken en verplichtingen gelden ten aanzien van de bescherming van persoonsgegevens. Om de interne marktbelemmeringen weg te nemen heeft de richtlijn een ruime werkingssfeer die vooral ziet op geautomatiseerde verwerkingen en niet de verwerkingen voor huishoudelijke en persoonlijke doeleinden. In hoeverre de werkingssfeer ook niet-geautomatiseerde verwerkingen omvat wordt deels overgelaten aan de nationale wetgever.

De richtlijn beoogt waar mogelijk tegemoet te komen aan de bijzonderheden van bepaalde categorieën van gegevens of verwerkingen of risico's en biedt de nationale wetgever in aangegeven gevallen de mogelijkheid om een eigen invulling te geven aan de wetgeving. De richtlijn beoogt ook dat zoveel mogelijk rekening kan worden gehouden met de specifieke omstandigheden en behoeften van de sector of branche. Daartoe beoogt de richtlijn te bevorderen dat op branche- en sectorniveau gedragscodes worden opgesteld.

---

[64] Overw. 27 richtlijn.
[65] Overw. 4, 6 en 8 richtlijn.

Om te komen tot een hoog beschermingsniveau beoogt de richtlijn de transparantie van gegevensverwerkingen te verbeteren door te voorzien in waarborgen voor betrokkenen. Deze bestaan uit verplichtingen voor verantwoordelijken en aanspraken voor betrokkenen. De richtlijn beoogt naleving van de privacywet te verzekeren door te voorzien in een onafhankelijke toezichthouder en toegang tot de rechter, alsmede door passende sancties. Met name waar het gaat om de meldplicht beoogt de richtlijn te voorkomen dat verantwoordelijken te maken hebben met onnodige uitvoeringskosten. Ten slotte beoogt richtlijn zoveel mogelijk technologie-onafhankelijke wetgeving, zodat bescherming gewaarborgd blijft als er zich technologische ontwikkelingen voordoen.

Hoofdstuk 3: Doelstellingen van de Wbp

3.1 Inleiding

Dit hoofdstuk betreft het tweede deel van de doelstellingeninventarisatie. Er wordt geïnventariseerd welke bedoelingen de nationale wetgever heeft gehad met de Wbp. Het uitgangspunt daarbij is uiteraard is dat de wetgever voortbouwt op de richtlijn die, zoals in het vorige hoofdstuk bleek, op haar beurt weer voortbouwt op het Verdrag inzake gegevensbescherming.[66] De doelstellingen van de richtlijn, waaronder die van het verdrag, worden dan ook gezien als doelstellingen van de Wbp.

In dit hoofdstuk wordt onderscheid gemaakt tussen enerzijds formele doelstellingen, die liggen in het voldoen aan verplichtingen op grond van hogere regelingen, en anderzijds materiële doelstellingen, die betrekking hebben op wijze waarop invulling is gegeven aan het realiseren van deze formele doelstellingen. Voor deze materiële doelstellingen is uiteraard bepalend in hoeverre de desbetreffende hogere regeling de nationale wetgever de ruimte laat om een eigen invulling te geven. Waar deze ruimte er niet is heeft de wetgever geen andere keus dan het uitvoering geven aan de desbetreffende voorschriften. En dat betekent dat er dan evenmin ruimte is voor eigen, van die van de gemeenschapswetgever te onderscheiden doelstellingen.

De belangrijkste bronnen voor dit onderdeel van de literatuurstudie zijn de parlementaire geschiedenis van de Wbp en in verband daarmee de evaluaties van de voorganger van de wet, de Wet persoonsregistraties (WPR).[67]

3.2 Formele doelstellingen

De nationale wetgever beoogt met de Wbp te voldoen aan de verplichtingen waaraan hij is gebonden op grond van hogere regelingen. Het gaat dan om de verplichtingen voortvloeiend uit het EG-Verdrag en de privacy-richtlijn, het Verdrag inzake gegevensbescherming en artikel 10, tweede en derde lid, van de Grondwet.

3.2.1 Implementatie privacy-richtlijn

De parlementaire geschiedenis van de wet laat er geen twijfel over bestaan wat de belangrijkste formele doelstelling van de Wbp is. In de memorie van toelichting (MvT) wordt kort en bondig gesteld:

> 'Het onderhavige voorstel voor een nieuwe Wet bescherming persoonsgegevens [...] strekt tot de implementatie van de richtlijn.'[68]

Het is duidelijk dat de doelstellingen van de richtlijn daarmee ook moeten worden gezien als doelstellingen van de wet. Daarbij kan worden opgemerkt dat de MvT deze doelstellingen van de richtlijn zelf inkleurt en dan soms wat verder gaat dan wat met zoveel woorden uit de richtlijn of preambule daarvan blijkt. Zo wordt in de MvT gesteld dat de richtlijn is opgesteld:

---

[66] Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg 28 januari 1981 (*Trb.* 1988, 7 en 1993, 11 (ratificatie)). Zie over de doelstellingen en inhoud van dit verdrag, dat door Nederland in 1993 werd geratificeerd: Berkvens & Prins 2000, p. 170-171.

[67] Overkleeft-Verburg 1995 en Prins e.a. 1995.

[68] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 5.

> '[m]et het het oog op de totstandbrenging van de informatiemaatschappij in de interne markt'.[69]

Ook wordt in de MvT aangetekend dat de richtlijn is gericht op het 'behouden van het vertrouwen van de consument' als deze gebruik gaat maken van 'de elektronische snelweg'. Deze overwegingen zijn evenwel niet terug te vinden in de tekst en de preambule van de richtlijn, maar lijken te zijn ontleend aan het zgn. Bangemann-rapport over 'Europe and the global information society',[70] waarnaar de MvT op dezelfde bladzijde verwijst.[71]

Over de te realiseren harmonisatie merkt de MvT op dat de richtlijn niet leidt tot een volledige harmonisatie van de privacywetgeving, maar een zekere bandbreedte biedt aan de lidstaten: er is een zeker minimum en een maximum dat niet mag worden overschreden. Binnen dit kader zijn de lidstaten vrij hun wetgeving in te richten.[72] Ook wijst de MvT op artikel 5 van de richtlijn, waarin lidstaten worden opgedragen om binnen de grenzen van Hoofdstuk II (d.w.z. art. 5 t/m 21) van de richtlijn nader de voorwaarden te bepalen waaronder de verwerkingen van persoonsgegevens rechtmatig zijn.

Voor de invulling van een en ander is gekozen voor wat wordt aangeduid als een 'genuanceerde benadering'.[73] Deze houdt kort gezegd in dat de precisering en concretisering gedeeltelijk in de wet heeft plaatsgevonden en daarnaast op andere wijzen wordt gerealiseerd. Voor de andere wijzen van concretisering en precisering wordt allereerst gedacht aan het stellen van nadere voorwaarden in sectorale wetgeving ten aanzien van het verwerken van persoonsgegevens, wat het mogelijk maakt om aan te sluiten bij de behoefte in meer op een bepaalde sector gerichte nadere regelgeving. Verder kan nadere concretisering van de door de richtlijn verlangde normering plaatsvinden door zelfregulering, ofwel in gedragscodes en reglementen. En verder zal, zo stelt de MvT, de concretisering van de Wbp ook tot ontwikkeling moeten komen in de jurisprudentie.[74]

De Wbp beoogt de richtlijn te implementeren en binnen de door de richtlijn gegeven bandbreedte gedeeltelijk nadere invulling te geven aan de voorwaarden waaronder verwerkingen rechtmatig zijn. Een nadere concretisering van de normen moet plaatsvinden in sectorale wetgeving en zelfregulering, alsmede in de jurisprudentie.

3.2.2 Uitvoeren artikel 10, tweede en derde lid, GW

In artikel 10, eerste lid, van de Grondwet (GW) staat dat iedereen behoudens bij of krachtens de wet te stellen beperkingen recht heeft op eerbiediging van zijn of haar persoonlijke levenssfeer. In het tweede lid wordt de wetgever opgedragen regels te stellen ter bescherming van de persoonlijke levenssfeer in verband met de vastlegging en verstrekking van persoonsgegevens. En in het derde lid wordt de wetgever opgedragen regels te stellen inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en het gebruik dat daarvan wordt gemaakt, alsmede de verbetering van deze gegevens. Met de Wbp beoogt de wetgever ook uitvoering te geven aan deze opdracht. De wet beoogt, evenals zijn voorganger de WPR, te voorzien in de door artikel 10, tweede en derde lid, GW verlangde regels:

---

[69] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 3.
[70] Europe and the global information society - Recommendations to the European Council, Brussel, 26 mei 1994 <http://europa.eu.int>.
[71] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 3.
[72] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 5-6.
[73] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 6.
[74] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 6; *Kamerstukken II* 1998–1999, 26 410, nr. 3, p. 2.

> 'De WPR en het onderhavige wetsvoorstel als opvolger van deze wet, vloeien voort uit de opdracht in de Grondwet tot het geven van deze regels'.[75]

Van belang daarbij is dat het derde lid van het grondswetsartikel niet zoals het tweede lid verwijst naar het recht op bescherming van de persoonlijke levenssfeer, maar verlangt dat er regels worden gesteld, ook als dat niet nodig zou zijn voor de bescherming van de persoonlijke levenssfeer.[76] Als zodanig niet in de parlementaire geschiedenis genoemd is dat de Wbp, evenals de WPR, in voorkomende gevallen de wettelijke grondslag kan bieden die artikel 10, eerste lid, GW verlangt voor een inbreuk op het in dat artikel vastgelegde recht op eerbiediging van een persoonlijke levenssfeer.[77]

De Wbp beoogt uitvoering te geven aan de opdracht van de grondwetgever om regels te stellen in verband met de vastlegging en verstrekking van persoonsgegevens, inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en het gebruik dat daarvan wordt gemaakt, en de verbetering daarvan.

3.2.3 Uitvoering Verdrag inzake gegevensbescherming

Evenals zijn voorganger, de WPR, strekt de Wbp tot uitvoering van het Verdrag inzake gegevensbescherming. De MvT zegt het zo:

> "Naast artikel 8 EVRM geven de WPR en de Wbp ook uitvoering aan het op artikel 8 EVRM steunende Verdrag inzake gegevensbescherming.[78]

Dat de wet uitvoering geeft aan het Verdrag inzake gegevensbescherming volgt ook uit de bedoeling van de richtlijn om de privacybeginselen van dit verdrag te verduidelijken en te versterken. Verder vloeit het ook voort uit de wens dat de Wbp zoveel mogelijk aansluit bij de WPR,[79] welke voorganger van de wet uitvoering gaf aan het verdrag.[80] Maar uit het zo even aangehaalde citaat uit de MvT lijkt ook te moeten worden opgemaakt dat de wet ook beoogt uitvoering te geven aan artikel 8 EVRM. Wat daarmee wordt bedoeld is niet helemaal duidelijk – het desbetreffende artikel legt het privacyrecht vast maar verlangt op zichzelf niet dat er in nadere wetgeving wordt voorzien. Bedoeld zal wellicht zijn dat de Wbp mede strekt tot bescherming van het in dit artikel vastgelegde recht op eerbiediging van de persoonlijke levenssfeer en dat de wet beoogt aan te sluiten bij de jurisprudentie van het Europees Hof voor de Rechten van de Mens in relatie tot de opslag en het gebruik van persoonsgegevens.[81] Ook denkbaar is wordt bedoeld dat de Wbp, evenals de WPR, in voorkomende gevallen de wettelijke grondslag kan bieden die artikel 10, eerste lid, GW verlangt voor een inbreuk op het in dat artikel vastgelegde privacyrecht.[82]

---

[75] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 7; zie voor een uitgebreidere bespreking van artikel 10, eerste tweede en derde lid, van de Grondwet: Koekkoek 2000, p. 155-178.
[76] Nadat de Raad van State negatief had geadviseerd over wetsvoorstellen tot wijziging van onder andere artikel 10 Gw heeft de regering eind 2004 aangekondigd nieuwe wetsvoorstellen tot wijziging van onder meer deze grondwetsbepaling te gaan voorbereiden. Bij brief van 18 november 2005 aan de Tweede Kamer heeft de regering dat eens nog bevestigd. Een en ander betekent dat op termijn een grondwetvoorstel voor een nieuw artikel 10 Grondwet kan worden verwacht. Het is niet uitgesloten, maar misschien ook niet heel waarschijnlijk, dat dit gevolgen kan hebben voor de Wbp. Omdat op dit moment niet duidelijk is wat de stand van zaken is, wordt daarop in dit onderzoek niet verder ingegaan.
[77] Zie Overkleeft-Verburg 1995, p. 30.
[78] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 8.
[79] Zie bijv. *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 5.
[80] *Kamesrtukken II* 1986-87, 19 095, nr. 3.
[81] Vgl. *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 7-8.
[82] Zie Overkleeft-Verburg 1995, p. 30.

De Wbp beoogt uitvoering te geven aan het Verdrag inzake gegevensbescherming en aan te sluiten bij de jurisprudentie van het EHRM over artikel 8 EVRM.

3.3 Materiële doelstellingen

De materiële doelstellingen van de wet betreffen de wijze waarop de formele doelstellingen zijn gerealiseerd. Het gaat dan om de keuzes die de nationale wetgever, voorzover de richtlijn hem daartoe de ruimte geeft, heeft gemaakt met betrekking tot de wijze waarop hij de richtlijn heeft geïmplementeerd.

3.3.1 Werkingssfeer en toepassing

Waar het gaat om de werkingssfeer en reikwijdte van de wet heeft de Nederlandse wetgever binnen de grenzen van de richtlijn een aantal keuzes gemaakt.

Aansluiten bij de WPR

De wetgever heeft ervoor gekozen om zoveel mogelijk aan te sluiten bij de WPR. Het uitgangspunt van de wetgever, dat door Nederland ook al naar voren is gebracht toen de richtlijn werd opgesteld, [83] is dat de Wbp niet minder bescherming moet bieden dan de WPR– dit in overeenstemming met de doelstelling van de gemeenschapswetgever dat de richtlijn een hoog beschermingsniveau beoogt en ernaar streeft de privacybeginselen van het Verdrag inzake gegevensbescherming te verduidelijken en te versterken.[84] Dit uitgangspunt heeft er onder andere toe geleid dat de wetgever, gebruikmakend van de ruimte die de richtlijn hem daartoe biedt,[85] bij de omschrijving van de voor de reikwijdte van de wet bepalende begrippen nadrukkelijk aansluiting heeft gezocht bij de begrippen van de WPR. Zo sluit het begrip 'persoonsgegeven' in artikel 1 Wbp inhoudelijk aan op de omschrijving die in de WPR werd gehanteerd, namelijk een gegeven dat herleidbaar is tot een individueel natuurlijk persoon, waar de Wbp uitgaat van een gegeven betreffende geïdentificeerde of identificeerbare natuurlijke personen.

Waar de nationale wetgever lijkt af te wijken van wat de gemeenschapswetgever beoogt is de invulling van het criterium van de identificeerbaarheid. In de preambule van de richtlijn wordt daarover opgemerkt, dat er moet worden gekeken:

> 'naar alle middelen waarvan redelijkerwijs mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om de genoemde persoon te identificeren'.[86]

Voor de gemeenschapswetgever gaat het dus om de middelen waarover de verantwoordelijke of 'enige ander persoon' kunnen beschikken. De indruk bestaat dat de nationale wetgever daarvan enigszins van heeft af willen wijken, niet zozeer in tekst van de wet maar in de MvT. Hoewel de zo even aangehaalde overweging uit de richtlijn integraal in de MvT wordt geciteerd gaat de MvT verder vooral uit van de middelen waarover de verantwoordelijke zelf beschikt.[87]

Ook bij de omschrijving van het begrip 'bestand' wordt aansluiting gezocht bij de WPR. Het begrip wordt op dezelfde wijze gedefinieerd als het begrip 'persoonsregistratie' uit de WPR:

---

[83] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 5-6.
[84] Zie par. 2.3.2 van dit rapport.
[85] Overw. 27 richtlijn.
[86] Overw. 26 richtlijn.
[87] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 47-49.

> 'Wat handmatige verwerkingen betreft komt de reikwijdte van het begrip "bestand" overeen met die van het begrip "persoonsregistratie" in de WPR.'[88]

Het bestandsbegrip heeft dus in de Wbp betrekking op verschillende personen, en omvat niet, zoals de definitie in de richtlijn, ook een gegevensverzameling met gegevens over een enkele persoon. Het advies van de Registratiekamer om het 'verschillende personen-vereiste' niet in de definitie op te nemen, heeft de wetgever uitdrukkelijk niet overgenomen. Dit omdat de reikwijdte van het begrip volgens de wetgever, 'thans in de jurisprudentie enigszins [is] uitgekristalliseerd', en omdat 'het onwenselijk [is] daarin weer wijziging te brengen'.[89] De wetgever kiest derhalve voor continuïteit en beperkt daarmee de reikwijdte van de wet voorzover het gaat om niet-geautomatiseerde verwerkingen of bestanden.

Voorzover mogelijk binnen de door de richtlijn gegeven ruimte beoogt de Wbp niet minder bescherming te bieden dan de WPR. De Wbp beoogt waar mogelijk uit te gaan van het begrippenkader van de WPR, teneinde gebruik te kunnen maken van de in het kader van deze wet ontwikkelde jurisprudentie.

Algemene toepassing tenzij anders bepaald in sectorale wetgeving

Waar het gaat om toepassing van de wet is het uitgangspunt is dat de wet van toepassing is tenzij er in desbetreffende sectorale wet is bepaald dat dit anders is geregeld.

> 'Deze keuze brengt met zich dat ook bij eventuele toekomstige wetgeving bevattende een uitputtend regime voor de bescherming van persoonsgegevens in een bepaalde sector, het niet van toepassing zijn van de Wbp in deze laatste wet zelf wordt vermeld. Deze keuze voorkomt vragen over de verhouding tussen verschillende wettelijke systemen.'[90]

Om vragen over de verhouding tussen de Wbp en sectorale wetten te voorkomen gaat de wet uit van het uitgangspunt dat de wet van toepassing is, tenzij er in een sectorale wet anders is bepaald.

Geen onderscheid in verband met verwerkingen die niet onder de richtlijn vallen

Bij het bepalen van de werkingssfeer van de wet heeft de wetgever ervoor gekozen om de twijfels die verband houden met de werking van het gemeenschapsrecht zoveel mogelijk te voorkomen. In artikel 3, tweede lid, eerste gedachtestreepje, van de richtlijn is over de werkingssfeer van de richtlijn bepaald dat verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat en de activiteiten van de Staat op strafrechtelijk gebied, niet onder het bereik van de richtlijn vallen. Zoals gezegd houdt dat verband met de juridische grondslag van de richtlijn, te weten artikel 100A EG-Verdrag (thans vernummerd naar 95 EG-Verdrag), dat ziet op harmonisatie met het oog op de totstandkoming van de interne markt en geen grondslag biedt voor verdergaande maatregelen.[91]

Voor zover het gaat om activiteiten die niet vallen onder de werkingssfeer van de richtlijn is de nationale wetgever vrij de wetgeving naar eigen inzicht in te richten en kan hij desgewenst de werkingssfeer van de wet uitbreiden, althans voorzover hij daarbij blijft binnen de kaders van het Verdrag inzake gegevensbescherming. In dat verband wordt in de MvT opgemerkt dat de reikwijdte van het communautaire of gemeenschapsrecht 'inherent dynamisch' is – dit omdat de organen van de Gemeenschap de opdracht hebben om het dat gemeenschapsrecht uit te breiden en aan te passen ter verwezenlijking van onder meer de interne markt. Als gevolg daarvan, volgens de MvT, verandert de scheidslijn tussen het nationale en het

[88] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 52; *Kamerstukken II* 1998-1999, 25 892, nr. 8, p. 13.
[89] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 54; zie ook *Kamerstukken II* 1997–1998, 25 892, A, p. 2-3.
[90] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 13.
[91] Vgl. EHvJ 30 mei 2006, zaken C-317/04 en C-318/04.

gemeenschapsrecht voortdurend. En dit kan tot twijfel over de werkingssfeer van de wet aanleiding geven.[92]

In de wet heeft de nationale wetgever ervoor gekozen om deze twijfel zoveel mogelijk te voorkomen door waar mogelijk geen betekenis toe te kennen aan het onderscheid tussen de gegevensverwerking die wel en niet onder het gemeenschapsrecht vallen. Dit is alleen anders als er aanleiding is om op onderdelen die niet onder het gemeenschapsrecht vallen, af te wijken van de algemene regels van de richtlijn.[93]

De Wbp beoogt voor zover mogelijk geen onderscheid te maken tussen verwerkingen die wél en verwerkingen die niet onder het gemeenschapsrecht vallen.

Journalistieke, artistieke en literaire doeleinden

Voorzover het gaat om de verwerking van gegevens voor uitsluitend journalistieke of voor artistieke of literaire doeleinden verlangt de richtlijn in artikel 9 dat lidstaten voorzien in uitzonderingsbepalingen die nodig zijn om het recht op een persoonlijke levenssfeer te verzoenen met de regels betreffende de vrijheid van meningsuiting.[94] Deze uitzonderingen mogen betrekking hebben op de regels van de hoofdstuk II, IV en VI van de richtlijn, zijnde de bepalingen over de rechtmatigheid van gegevensverwerkingen (art. 6 t/m 24 Wbp), doorgifte naar derde landen (art. 76 t/m 78 Wbp) en de uitzonderingen en beperkingen (art. 43 Wbp).

Anders dan in de WPR kon de wetgever de verwerkingen voor journalistieke doeleinden (eigenlijk: persoonsregistraties die uitsluitend ten dienste staan van de openbare informatievoorziening door pers, radio of televisie)[95] dus niet geheel uitzonderen van de werking van de wet. Vanwege de grote betekenis van de vrijheid van meningsuiting is ervoor gekozen om de Wbp niet onverkort van toepassing te laten zijn op journalistieke activiteiten. Uitgesloten zijn de meldings- en informatieverplichtingen, en kennisneming-, verbetering- en verzetsrechten, alsmede de bevoegdheden van de Cbp om bijvoorbeeld voorafgaand onderzoek te doen. Evenmin is van toepassing het verwerkingsverbod dat geldt ten aanzien van bijzondere gegevens, zoals de gegevens betreffende geloofsovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven enz. Wel van toepassing zijn evenwel de algemene beginselen inzake gegevensverwerkingen.[96] Verder zijn de regels van toepassing waarvoor de richtlijn geen uitzondering toestaat, te weten de regels inzake aansprakelijkheid, sancties, beroep op de rechter, gedragscodes en beveiliging.[97]

Op deze wijze beoogt de wetgever een evenwicht te bewerkstelligen tussen enerzijds privacybescherming en andere grondrechten, meer in het bijzonder de vrijheid van meningsuiting. En daarbij beoogt de wetgever nadrukkelijk aan te sluiten bij de jurisprudentie hierover.[98]

De Wbp beoogt een evenwicht te bewerkstelligen tussen privacybescherming en andere grondrechten, meer in het bijzonder de vrijheid van meningsuiting. Daarbij beoogt de wet aan te sluiten bij de jurisprudentie hierover.

[92] Vgl. EHvJ 30 mei 2006, zaken C-317/04 en C-318/04.
[93] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 14.
[94] Overw. 37 richtlijn.
[95] Art. 2, onder a, WPR.
[96] Resp. art. 6 en 7 richtlijn.
[97] Zie Kabel 1997, p. 76-80.
[98] *Kamerstukken II* 1997-1998, 25 892, nr. 8, p. 55-57; *Kamerstukken I* 1999–2000, 25 892, nr. 92c, p. 18.

3.3.2 Normatieve kaders

Open normen en belangenafwegingen

Waar het gaat om de voorwaarden waaronder een gegevensverwerking rechtmatig is biedt de richtlijn niet veel ruimte voor een eigen invulling van de nationale wetgever. Op advies van onder andere de Registratiekamer en ondernemers- en werkgeversorganisaties heeft de wetgever er bewust voor gekozen om dicht bij de bij de tekst van de richtlijn te blijven. Als gevolg daarvan gaat de Wbp, evenals de WPR, uit van veel normen die als vaag of open zijn te typeren.

De redenen daarvoor houden allereerst verband met het ruime toepassingsbereik van de wet, waardoor de praktijk niet met de wet uit de voeten zou kunnen als precies wordt vastgelegd wat wel mag en wat niet mag. De wet is dan ook terughoudend met het preciseren en laat dat zoveel mogelijk over aan zelfregulering binnen de door de wet gegeven kaders.[99] De wet geeft dan ook niet steeds eenduidige gedragsvoorschriften, maar schrijft voor op welke wijze welke belangen moeten worden afgewogen en welke maatstaven daarbij relevant zijn.

> 'De wet beoogt de voor de verwerking relevante belangen en de criteria waaraan moet worden getoetst uitdrukkelijk in beeld te brengen'.[100]

Over de vaagheid van de normen worden in de MvT verbanden gelegd met de ontwikkelingen van de informatietechnologie en de turbulente context die daarvan het gevolg is, voor een deel onvermijdelijk. Dit maakt dat de wet wel moet uitgaan van vage en open normen:

> 'de technische ontwikkelingen [stellen] het recht voor uitdagingen [..] die slechts door de geleidelijke ontwikkeling van nieuwe rechtsbegrippen en daarmee verbonden rechten sui generis het hoofd kunnen worden geboden. Een uitgekristalliseerd juridisch begrippenapparaat en een heldere, dat wil zeggen vaststaande invulling daarvan in de juridische dogmatiek, zal pas beschikbaar zijn wanneer ook de informatietechnologische ontwikkelingen in een rustiger vaarwater zijn gekomen. Wij onderschrijven evenwel dat ook onder deze omstandigheden de regels zo helder mogelijk moeten zijn. Willen de regels echter meer zijn dan vrijblijvende, vrome beginselen, zonder de gerechtvaardigde gegevensverwerkingen onnodig te beperken, dan valt niet te ontkomen aan begrippen die een daadwerkelijk kristallisatiepunt voor rechtspraktijk en jurisprudentie kunnen zijn, met alle daaraan inherente rechtsonzekerheid'.[101]

Opmerkingen van deze strekking worden meerdere keren gemaakt in de MvT. Aangenomen wordt dan ook dat de wet uitdrukkelijk beoogt te voorzien in dergelijk kristallisatiepunten.[102]

De wet beoogt te voorzien in begrippen die een kristallisatiepunt bieden voor nadere rechtsvorming in de rechtspraktijk en de jurisprudentie. In verband daarmee beoogt de wet door middel van open en vage normen te voorzien in het instrumentarium voor de afweging van de bij gegevensverwerkingen betrokken belangen.

Open normen en inbedding in het rechtsstelsel

In de MvT worden deze vage en open normen, zoals het rechtvaardig belang van de verantwoordelijke of de onverenigbaarheid van verwerkingsdoeleinden,[103] ook in verband gebracht met de kritiek over de ge-

---

[99] *Handelingen II* 18 november 1999, p. 24-791 en 24-792.
[100] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 15.
[101] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 40.
[102] *Kamerstukken II* 1998-1999, 25 892, nr. 6, p. 14.
[103] Resp. art. 8, onder f, en 9, eerste lid, Wbp.

brekkige inbedding van privacywetgeving in het rechtsstelsel. Deze gebrekkige inbedding was gebleken uit de evaluaties van de WPR,[104] waarin was vastgesteld dat deze wet maar in beperkte mate aansloot op andere wetgeving. Dit werd ondersteund door het gegeven dat er weinig jurisprudentie op grond van deze wet was. De bescherming van persoonsgegevens bleek veelal niet via de WPR te worden vormgegeven, maar op basis van het civiele recht of in de publieke sector via de beginselen van behoorlijk bestuur of de Wet openbaarheid van bestuur (Wob). In reactie op deze evaluatie van de WPR verwijst de MvT naar het karakter van de wet. In veel gevallen kan de wet volgens de MvT niet voorzien in een sluitend stelsel van concrete materiële normen over wat wel en wat niet zou mogen bij de verwerking van persoonsgegevens. De wet bevat daarom veel open of vage normen. En die geven niet zozeer antwoorden op op het concrete geval toegespitst vragen, maar vormen vooral een 'kristallisatiepunt' voor jurisprudentie en nadere sectorale wetgeving.[105] Maar dat hoeft volgens de wetgever op zichzelf niet in de weg te staan aan een goede inbedding van de wet. In de MvT wordt in verband daarmee gesproken over het 'kameleontisch karakter' van de belangenafwegingen die de wet voorschrijft:

> 'De bepaling inzake de afweging van belangen heeft in zoverre een kameleontisch karakter dat de toets in rechte achteraf of een aanvaardbare afweging heeft plaatsgevonden zich kleurt naar gelang het gaat om een gegevensverwerking in de publieke, dan wel in de private sector. In het eerste geval wordt getoetst of bij de afweging is voldaan aan de bestuursrechtelijke beginselen van behoorlijk bestuur; in het tweede geval of de zorgvuldigheid die volgens het ongeschreven recht in het maatschappelijk verkeer betaamt'.[106]

Afhankelijk van de context waarbinnen de verwerkingen plaats vinden gaat de Wbp dus uit van bestuursrechtelijke beginselen of van normen uit het burgerlijk recht. In dat verband wijst de MvT er op dat de Wbp voorziet in een gedifferentieerd stelsel van rechterlijke toetsing. Op de beslissingen die binnen de overheid worden genomen over gegevensverwerkingen is de Algemene wet bestuursrecht (Awb) van toepassing en is de bestuursrechter bevoegd. In de private sector wordt getoetst aan de in het burgerlijke recht geldende maatstaven en is de civiele rechter bevoegd. Het gevaar voor uiteenlopende jurisprudentie acht de MvT niet groot omdat in beide gevallen de concretisering van de open normen plaatsvindt tegen de achtergrond van de algemene noties die in het bestuursrecht en in het civiele recht gelden. Wel wordt aangegeven dat daarmee een betere inbedding in het rechtsstelsel wordt gerealiseerd. En dit omdat in dit geval de invulling van de open normen van de wet niet zozeer voortkomt uit de privacywet maar uit het bestuursrecht:

> 'De nadere invulling van materiële normen [..] krijgt door de verschillende jurisprudentie gestalte [..]. De afbakening is dan evenwel niet één die eigen is aan het privacyrecht, doch is er één van de Awb. Aldus vindt wederom een betere inbedding in het overige recht plaats'.[107]

Daarnaast worden ook andere maatregelen genoemd om een beter inbedding van de wet te bereiken. Zo wordt ook het versterken van de rechtspositie van de verantwoordelijke, door deze in staat te stellen sommige beslissingen van de toezichthouder in rechte aan te vechten, gezien als een maatregel gericht op een betere inbedding in het rechtsstelsel.[108] Als instrumenten om deze betere inbedding te bereiken noemt de MvT verder de vanuit verschillende rechtsgebieden te concretiseren open normen en de gedifferentieerde rechterlijke toetsing. In dat verband kan ook worden genoemd de wijze waarop wordt bepaald wie de verantwoordelijke is. Daarbij gaat de Wbp, anders dan de WPR, uit van de formeel juridische criteria die aansluiten bij de onderscheiden rechtsgebieden.

---

[104] Overkleeft-Verburg 1995 en Prins e.a. 1995.
[105] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 37.
[106] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 38.
[107] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 39.
[108] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 26.

De Wbp beoogt ingebed te zijn in het rechtsstelsel en beter (dan de WPR) aan te sluiten bij overige wetgeving, door het gebruik van open normen die vanuit verschillende rechtsgebieden kunnen worden geconcretiseerd en door de versterking van de rechtspositie van de verantwoordelijke.

Verduidelijken geadresseerde-begrip

Waar het gaat om de (belangrijkste) geadresseerde in de wet, de verantwoordelijke, heeft de wetgever ervoor gekozen om af te wijken van de WPR en aan te sluiten bij bestaande privaatrechtelijke en publiekrechtelijke verhoudingen, omdat deze voor de betrokkenen beter kenbaar zijn dan de in de WPR gehanteerde zeggenschapscriterium.[109] De wet beoogt daarmee onduidelijkheden over wie de verantwoordelijke is op te helderen en daarmee problemen te voorkomen over wie kan worden aangesproken over de wettelijke verplichtingen en aanspraken. De MvT spreekt in dat verband over 'een van de algemene doelstellingen van het informaticarecht' die erop is gericht om:

> 'de situatie te vermijden dat personen schade ondervinden van geautomatiseerde gegevensverwerking zonder dat een ander rechtssubject daarop aanspreekbaar is.'

Wat dat betreft beoogt de wet dus ook de positie van de betrokkene te verbeteren en hem beter in staat te stellen om de wettelijke bescherming te effectueren. Daarnaast kan ook dit worden gezien als een middel dat ertoe bijdraagt dat de Wbp beter is ingebed in het rechtstelsel. [110]

De Wbp beoogt de positie van de betrokkenen te versterken door onduidelijkheden over het verantwoordelijke-begrip op te helderen en aan te sluiten bij bestaande privaatrechtelijke en publiekrechtelijke verhoudingen.

Aansluiten bij risico's van gegevensverwerkingen

Een van de uitkomsten van de evaluaties van de WPR was de aanbeveling dat de privacyregulering zou moeten aansluiten bij potentiële risico's van gegevensverwerking, en niet bij maatschappelijke sectoren waar de gegevensverwerkingen plaatsvinden. Volgens de MvT biedt de richtlijn verschillende mogelijkheden om daaraan uitvoering te geven. De MvT wijst er daarbij allereerst op dat de wet waar het gaat om de materiële normen voor de publieke en de private sector uitgaat van dezelfde regels. Verder wijst de MvT erop dat de wet specifieke regels stelt met betrekking tot de verwerking van gevoelige of bijzondere gegevens die naar hun aard een groter risico voor de persoonlijke levenssfeer betekenen, zoals gezondheidsgegevens of gegevens met betrekking tot geloofsovertuiging of ras. Ook wordt verwezen naar de bevoegdheid van de toezichthouder om voorafgaand onderzoek te doen naar gegevensverwerkingen die een bijzonder risico opleveren voor de persoonlijke levenssfeer van de betrokkene.[111]

De Wbp beoogt waar mogelijk aan te sluiten bij potentiële risico's van gegevensverwerkingen en niet zozeer bij de maatschappelijke sectoren waar de verwerkingen plaatsvinden.

Waarborgen privacy- en andere grondrechten

De Wbp beoogt te voorzien in waarborgen ter bescherming van het recht op eerbiediging van de persoonlijke levenssfeer in relatie tot de verwerking van persoonsgegevens. In aanvulling daarop wordt in de MvT aangegeven dat de wet ook een ondersteunende rol beoogt te hebben bij het waarborgen van andere grondrechten. Als voorbeeld daarvan wordt in de MvT allereerst het gelijkheids- of non-discriminatiebeginsel genoemd, waarbij de wet een ondersteunende functie heeft. In dat verband wijst de MvT erop dat

---

[109] *Kamerstukken II* 1997-1998, 25 892, nr. 8, p. 55-56.
[110] Zie par. 3.2.1 t/m 3.2.3 van dit rapport.
[111] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 40-41, 125-128, 144.

de regeling met betrekking tot de verwerking van bijzondere persoonsgegevens (betreffende onder meer iemands godsdienst of levensovertuiging, ras, politieke gezindheid en seksuele leven) ook kan worden gezien als uitwerking of doorwerking van het verbod om onderscheid te maken tussen personen op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat. [112]

Onder verwijzing naar het wetgevingsadvies van de Registratiekamer wordt er in de MvT verder op gewezen dat een ongebreidelde (dus: niet overeenkomstige de normering van de wet uitgevoerde) verwerking van persoonsgegevens ook een negatieve uitwerking kan hebben de vrijheid van meningsuiting en politieke participatie en dergelijke. Daarbij wordt in het bijzonder gedacht aan:

> 'gevallen waarin een persoon of instantie over iemand zoveel gegevens met een zodanige lading heeft verzameld dat die persoon of instantie door het schermen met deze gegevens het gedrag van de betrokkene, waaronder ook het uitoefenen van grondrechten, kan beinvloeden.' [113]

Of de wetgever nog andere grondrechten op het oog heeft blijkt niet uit de MvT. Uitgaande van de in het citaat uitgedrukte chantage-dreiging lijken ook andere grondrechten die de handelingsvrijheid van individuen betreffen in aanmerking te komen, zoals de vrijheid van godsdienst en levensovertuiging (art. 6 GW), de vrijheid van vereniging (art. 8 GW) en de vrijheid van vergadering en betoging (art. 9 GW).[114]

Verder wijst de MvT erop dat de in de wet geregelde informatieplichten en kennisnemings- en andere rechten verband houden met het recht op toegang tot de rechter dat is vastgelegd in artikel 13 EVRM en artikel 17 van de Grondwet. Om zijn rechten met betrekking tot de verwerking van persoonsgegevens te kunnen effectueren en zonodig naar de rechter te kunnen stappen is nodig dat betrokkenen kennis kunnen hebben van deze verwerkingen. En omdat het niet vanzelfsprekend is dat betrokkenen kennis hebben van de verwerking van hun persoonsgegevens, worden compenserende wettelijke maatregelen nodig geacht. Daaronder worden ook de bevoegdheden van de toezichthouder begrepen.[115]

In aanvulling op de bescherming van privacy-grondrechten beoogt de Wbp waarborgen te bieden tegen verwerkingen van persoonsgegevens die afbreuk kunnen doen aan de werking van andere grondrechten, zoals met name het gelijkheid- of non-discriminatiebeginsel van artikel 1 Gw en andere grondrechten die betrekking hebben op de handelingsvrijheid van individuen.

3.3.3 Transparantie en rechten van betrokkenen

De positie van de betrokkene ten opzichte van de verantwoordelijke hangt af van bekendheid van de betrokkene met de gegevens die de verantwoordelijke over hem verwerkt. Wie niet weet of zijn of haar gegevens (onrechtmatig) worden verwerkt zal niet goed in staat zijn daaraan iets te doen. Van belang daarbij is dat de ontwikkeling van de informatiemaatschappij volgens de MvT leidt tot meer mogelijkheden van gegevensverwerking buiten de betrokkene om:

> 'Om de betrokkene effectief in staat te stellen zijn rechten te verwerkelijken, moet hij van de verwerking van hem betreffende gegevens op de hoogte zijn. De bedreiging van de persoonlijke levenssfeer in de informatiemaatschappij bestaat echter juist uit de vele mogelijkheden om persoonsgegevens buiten medeweten van de betrokkene te verwerken.'[116]

---

[112] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 8, 10-11; Zie ook Overkleeft-Verburg 1995, p. 26.
[113] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 8, 10-11.
[114] Overkleeft-Verburg 1995, p. 28-29.
[115] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 8.
[116] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 18.

Om deze reden stelt de Wbp meer nog dan de WPR voorwaarden die gericht zijn op het transparant maken van gegevensverwerkingen. Deze betreffen rechten voor betrokkenen en daarmee corresponderende verplichtingen voor verantwoordelijken ten opzichte van de betrokkenen. Daarnaast voorziet de wet in verplichtingen voor de verantwoordelijke, zoals de meldplicht, waarmee wordt beoogd de transparantie van gegevensverwerkingen voor 'toezichthoudende instanties en een breder publiek' te vergroten.[117] Ook hier legt de MvT een verband met dreigingen die zouden voortkomen uit de ontwikkeling van informatietechnologie. Deze ontwikkelingen leiden volgens de MvT er met name toe dat meer gegevens buiten de betrokkene om kunnen worden verwerkt:

> 'De toenemende informatietechnologische mogelijkheden tot manipulatie van persoonsgegevens maken de positie van de burger steeds kwetsbaarder. Het is voor de individuele burger zeer moeilijk greep te houden op de wijze waarop er met zijn persoonsgegevens wordt omgegaan. Dat hangt samen met het feit dat de verwerking van persoonsgegevens zich in belangrijke mate aan zijn waarneming onttrekt. Deze achtergrond rechtvaardigt de instelling van een overheidsorgaan met eigen bevoegdheden om de naleving van de wettelijke voorschriften en de rechtsontwikkeling op dit punt te bevorderen.[118]

De meldingsplicht wordt gezien als een middel te vergroting van de transparantie van verwerkingen ten opzichte van betrokkenen en de toezichthouder. In de MvT wordt dit, onder verwijzing naar de richtlijn, in relatie gebracht met de controleerbaarheid van de belangenafwegingen die moeten plaatsvinden als er sprake is van de verwerking van persoonsgegevens:

> 'Aanmelding heeft tot doel de transparantie van de gegevensverwerking te bevorderen. De handelingsvrijheid van een ieder om voor op zichzelf gerechtvaardigde doeleinden gegevens te verwerken, wordt ingeperkt door de grondwettelijk gewaarborgde vrijheid van de betrokkene om niet onnodig aan verwerking van hem betreffende gegevens te worden onderworpen. Dit leidt enerzijds tot het materiële voorschrift dat de belangen van de verantwoordelijke en de betrokkene tegen elkaar moeten worden afgewogen; anderzijds tot het procedurele voorschrift dat de afweging controleerbaar dient te zijn'.[119]

De meldplicht beoogt de transparantie van de gegevensverwerking te bevorderen en daarmee waarborgen te bieden om de afweging van de betrokken belangen controleerbaar te maken. In de toelichting bij het besluit waarin de vrijstellingen op de meldplicht worden geformuleerd, het Vrijstellingsbesluit,[120] wordt dit nader uiteengezet.[121] Er wordt allereerst aangegeven dat de meldplicht niet zozeer dient om de bescherming ten aanzien van de gegevensverwerking te verhogen maar veeleer beoogt verwerkingen voor de betrokkene controleerbaar te maken en de toezichthouder in staat te stellen beter zijn werk te doen, alsmede de verantwoordelijken aan te zetten zich rekenschap te geven van de doeleinden waarvoor en de wijze waarop gegevens worden verwerkt:

> 'De meldingsplicht dient de transparantie van de gegevensverwerking voor de betrokkene. Het maakt de gegevensverwerking voor hem controleerbaar. Als verwerkingen die geen risico opleveren van een inbreuk op de rechten en vrijheden van betrokkenen zijn vrijgesteld van de aanmeldingsplicht, is het Cbp beter in staat toezicht uit te oefenen op de gegevensverwerkingen waarbij een dergelijke risico niet bij voorbaat is uitgesloten. De meldingsplicht heeft mede tot doel dat de verantwoordelijke geprikkeld wordt om zich rekenschap te geven van de doeleinden waarvoor hij persoonsgegevens wil verwerken en

---

[117] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 15.
[118] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 26.
[119] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 132-133.
[120] *Stb.* 2004, 261.
[121] Zie ook par. 3.4 en 4.5 van dit rapport.

> verslag te doen van de overwegingen welke persoonsgegevens noodzakelijk zijn voor het bereiken van het doel en van het gebruik van de gegevens in verband met dat doel'. [122]

Het gaat om controleerbaarheid van verwerkingen voor betrokkenen, het verbeteren van toezicht door het Cbp en het prikkelen van de verantwoordelijke om in overeenstemming met de wet gegevens te verwerken. Uit deze functies van de meldplicht vloeit volgens de toelichting bij het besluit voort dat niet kan worden tegemoet gekomen aan het voorgestelde stelsel van een genormeerde meldplicht, waarbij het uitgangspunt is dat alleen de als zodanig aangeduide verwerkingen moeten worden gemeld en de rest automatisch is vrijgesteld. De toelichting stelt dat het stelsel van de genormeerde vrijstelling nodig is omdat daarin de vrijgestelde verwerkingen worden beschreven:

> Deze functies blijven behouden doordat de doelstelling, de aard van de gegevens en de verstrekkingen in de vrijstelling worden beschreven. De beantwoording van de vraag naar het doel van de verwerking ligt dan besloten in de toets van de verantwoordelijke of wel of niet moet worden aangemeld. De veronderstelling van het RCO in haar reactie als zou de meldingsplicht enkel gelden ten aanzien van gegevensverwerkingen waarvan de geboden bescherming, ondanks de werking van de Wbp, toch nog onvoldoende wordt geacht, is derhalve onjuist'.[123]

De keuze voor dit stelsel van de genormeerde vrijstelling mag, zo blijkt uit de MvT, er evenwel niet toe leiden dat de meldplicht op teveel verwerkingen van toepassing is. Want dan is er het risico dat de meer risicovolle verwerkingen worden ondergesneeuwd door de minder risicovolle verwerkingen, waardoor de transparantie van verwerkingen juist wordt verminderd:

> 'Indien aan de meldingsplicht onverkort de hand zou worden gehouden, zou afbreuk worden gedaan aan de daarmee beoogde transparantie. Er zouden vele gegevensverwerkingen moeten worden aangemeld waarvan het bestaan evident is. Het gevolg zou slechts zijn dat de gegevensverwerkingen waarvan het wel nodig is dat zij in beeld worden gebracht, ondersneeuwen. Het is daarom nodig de bekende, veel voorkomende vormen van gegevensverwerking waarvan het bestaan in het algemeen bekend mag worden verondersteld, van de meldingsplicht vrij te stellen'.[124]

De mogelijkheid om vrijstellingen op de meldingsplicht te formuleren dient dus mede het bevorderen van de transparantie van gegevensverwerkingen.

Om de positie van betrokkenen tegenover verantwoordelijken te versterken beoogt de Wbp de transparantie van gegevensverwerkingen te vergroten. De wet doet dit door rechten toe te kennen aan betrokkenen en daarmee corresponderende verplichtingen op te leggen aan verantwoordelijken, alsmede door het aan verantwoordelijken opleggen van een meldplicht en door het instellen van een privacytoezichthouder.

3.3.4 Zelfregulering

Door het mogelijk maken van zelfregulering beoogt de Wbp beter aan te sluiten bij de specifieke behoeften van een bepaalde organisatie, branche of sector. De MvT spreekt in dat verband over de concretisering en verdere invulling van het abstracte wettelijke normkader via zelfregulering.

---

[122] NvT Vrijstellingsbesluit, *Stb.* 2001, 250, p. 37.
[123] NvT Vrijstellingsbesluit, *Stb.* 2001, 250, p. 37.
[124] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 140.

> 'het [gaat] om een abstract normenkader dat door middel van [onder meer] zelfregulering (m.n. gedragscodes) zijn verdere invulling zal moeten krijgen'. [125]

Het gaat er daarbij om dat de wet het mogelijk maakt om te differentiëren afhankelijk van de context waarin de bescherming moet worden geboden. De wet voorziet daartoe in gedragscodes die door organisaties van verantwoordelijken op branche- of sectorniveau kunnen worden vastgesteld.[126] Een ander, in de wet geïntroduceerd zelfreguleringinstrument is het instituut van de functionaris voor de gegevensbescherming (FG). Verder worden ook de meldingen genoemd als middel om te bereiken dat de wet beter aansluit bij de specifieke situatie waarin de bescherming wordt geboden.

De Wbp beoogt dat de materiële normen via zelfregulering (gedragscodes, FG en meldingen) nader worden ingevuld. Zodoende beoogt de wet het mogelijk te maken dat wordt gedifferentieerd naar de context waarin de werkingen plaatsvinden.

Gedragscodes

De gedragscode is in de Wbp een belangrijk middel om aan te sluiten bij de specifieke behoeften van organisaties, branches en sectoren – afgaand op het aantal vermeldingen in parlementaire geschiedenis wellicht het belangrijkst geachte middel. De gedragscode betreft een vorm van collectieve zelfregulering. Om de opstelling van gedragscodes aan te moedigen beoogt de wetgever dan ook een aantal in de evaluaties van de WPR vastgestelde knelpunten weg te nemen. Dit betreft allereerst het afschaffen van de verplichting om betrokkenen de gelegenheid te bieden opmerkingen te maken over de gedragscode. Deze inspraakmogelijk bleek niet goed van de grond te zijn gekomen, met name omdat betrokkenen niet voldoende waren georganiseerd.

Ook heeft de wetgever getracht onduidelijkheid weg te nemen over de beroepsmogelijkheden tegen de beslissing van de toezichthouder over het al dan niet goedkeuren van een gedragscode. Door deze beslissing aan te merken als besluit in de zin van de Awb is duidelijk dat daartegen beroep bij de bestuursrechter mogelijk is. Aangenomen mag worden dat de Wbp daarmee ook beoogt de positie van verantwoordelijken en brancheorganisaties ten opzichte van het Cbp te verduidelijken cq. te verstevigen, zoals de MvT in meer algemene zin uitdrukt waar het gaat om de positie van verantwoordelijke tegenover het Cbp.[127] Over wat er in de gedragscodes zou moeten staan worden in de MvT opgemerkt dat er niet mag worden volstaan met het herhalen of papagaaien[128] van de bepalingen uit de wet,. Het is de bedoeling dat de gedragscode een nadere, op een bepaalde sector of branche gerichte invulling geeft van de open normen die de wet geeft voor de verwerking van persoonsgegevens. De gedragscode wordt dan ook geacht deze regels te preciseren naar gelang de sector waarvoor de code geldt.

> 'De algemene en flexibele normen van de wet dienen in een gedragscode een nauwkeuriger vertaling te krijgen in het licht van de desbetreffende sector. Dit komt ook de rechtszekerheid ten goede. Een gedragscode kan daarom niet volstaan met het grotendeels eenvoudig herhalen van een aantal wettelijke bepalingen. Dit laat onverlet dat desgewenst een aantal wettelijke bepalingen, indien deze zich in de desbetreffende sector niet goed lenen voor een nadere uitwerking, toch volledigheidshalve kunnen worden overgenomen. De code bevat dan binnen de sector een totaalbeeld van de geldende regels'.[129]

---

[125] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 16, zie ook p. 6 en 111.
[126] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 41.
[127] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 26-27 en 38.
[128] In dit verband wordt wel de term 'papagaaibepalingen' gebruikt, vgl. Overkleeft-Verburg 1995, p. 189.
[129] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 130.

De Wbp beoogt de opstelling van gedragscodes te bevorderen door de procedure te versimpelen (en bestaande inspraakmogelijkheden te schrappen). Verder beoogt de wet de positie van verantwoordelijken ten opzichte van het Cbp op te helderen door beroep bij de bestuursrechter open te stellen tegen beslissingen inzake de goedkeuring van gedragscodes.

Functionaris voor de gegevensbescherming (FG)

De functionaris voor de gegevensbescherming of FG is in Nederland geïntroduceerd door de Wbp. Het betreft een natuurlijke persoon die binnen de organisatie van de verantwoordelijke is belast met het toezicht op de verwerkingen van persoonsgegevens overeenkomstig de bepalingen van de Wbp. Ook met de invoering van het instituut van de FG beoogt de wetgever het mogelijk te maken dat beter kan worden aangesloten bij de specifieke behoeften van een bepaalde organisatie, branche of sector. Evenals de gedragscode maakt de FG 'maatwerk' mogelijk.

> 'De waarde van het nieuwe instituut is met name gelegen in de mogelijkheden om de uitoefening van taken en bevoegdheden van de Registratiekamer, onder behoud van haar positie, door deze functionaris te laten verrichten op een voor de desbetreffende organisatie, branche of sector geëigende wijze'.[130]

Anders dan de gedragscode betreft het instituut van de FG niet perse collectieve zelfregulering maar ook (en in de praktijk: vooral) individuele zelfregulering. De MvT spreekt in dat verband ook over de invulling van de eigen verantwoordelijkheid van verantwoordelijken, in welk verband met name wordt gewezen op de mogelijkheid om meldingen niet bij het Cbp te doen maar bij de eigen FG. De melding kan dan volgens intern te bepalen regels verlopen, wat door de verantwoordelijke minder 'als inmenging van buitenaf' zou worden ervaren.[131]

Verder beoogt de wet met het instituut van de FG iets te doen aan gebrekkige naleving van de meldingsplicht. De wet maakt het mogelijk dat verwerkingen worden gemeld bij de FG in plaats van bij het Cbp. Daarmee wordt, zo blijkt uit de MvT, ook beoogd de ontwikkeling van kennis en deskundigheid over gegevensbescherming te bevorderen. En ook daarmee wordt beoogd een bijdrage te leveren aan zelfreguleringinitiatieven:

> 'De gebleken problemen bij de aanmelding van persoonsregistraties bij de Registratiekamer, zijn mede aanleiding geweest in de richtlijn de mogelijkheid op te nemen om te melden bij een eigen toezichthouder. Daarmee wordt bovendien een verdere spreiding van de expertise inzake gegevensbescherming bevorderd, evenals de naleving van de meldingsplicht. De zelfregulering wordt hiermee gediend'.[132]

In dat kader wordt door de minister ook gewezen op het bevorderen van het privacybewustzijn en de deskundigheid op dat gebied.[133]

De Wbp beoogt door het instituut van de FG te komen tot een betere, meer omvattende invulling van de eigen verantwoordelijkheid van verantwoordelijken. Het maakt maatwerk mogelijk en wordt geacht de kennisontwikkeling over gegevensbescherming en privacybewustzijn te bevorderen.

Meldplicht

Ook de meldplicht wordt gezien als een middel waarmee zelfregulering kan worden ingevuld en bevorderd, hoewel dat in de Wbp minder evident is dan het was in de WPR waar de melding van verwerkingen

---

[130] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 29.
[131] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 41.
[132] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 39.
[133] *Handelingen I* 3 juli 2000, p. 34-1628.

nog echt het karakter had van zelfregulering op het niveau van de individuele verantwoordelijke. In de Wbp betreft de melding veeleer een beschrijving van de desbetreffende gegevensverwerking. Het gaat derhalve volgens de MvT meer om een procedurevoorschrift strekkende tot transparantie dan om een normering op het niveau van de individuele gegevensverwerking. Echter, de MvT voegt daaraan toe dat in de praktijk het verschil met de situatie onder de WPR, waar de meldplicht zonder meer strekte tot zelfregulering op een individueel niveau, niet groot zal zijn. Immers,

> '[h]et melden van een feitelijke beschrijving omtrent de wijze waarop de gegevens worden verwerkt, impliceert dat de verantwoordelijke in beginsel ook dienovereenkomstig zal moeten handelen'.[134]

De meldingsplicht komt er dus op neer dat de verantwoordelijke voor zichzelf regels stelt met betrekking tot de wijze waarop persoonsgegevens worden verwerkt. En daarmee kan ook de meldingsplicht worden gezien als een van de instrumenten waarmee beoogd wordt aan te sluiten bij de specifieke behoeften van een bepaalde verantwoordelijke. In zoverre kan de meldingsplicht worden gezien als zelfregulering op een het niveau van de verantwoordelijke. Daarnaast beoogt de meldplicht, zoals al bleek bij de bespreking van de transparantie in paragraaf 3.3.3, de transparantie van de gegevensverwerking te het bevorderen en daarmee waarborgen beoogt te bieden om de afweging van de betrokken belangen controleerbaar te maken.[135]

De meldplicht kan worden gezien als een middel om zelfregulering op het niveau van de verantwoordelijke. Met de melding beoogt de Wbp de verantwoordelijken in staat te stellen aan te sluiten bij hun eigen specifieke behoeften.

3.3.5 Toezicht en rechtsbescherming

Onafhankelijkheid en maatschappelijk draagvlak van het Cbp

Voor het toezicht op de naleving van de Wbp vertrouwt de wet, zoals ook de richtlijn, in vergaande mate op de onafhankelijke toezichthouder. De achterliggende reden ligt in de veronderstelling dat de naleving van de wet niet uitsluitend afhankelijk kan worden gesteld van het initiatief van de burger, die kennelijk geacht wordt daartoe onvoldoende in staat te zijn. En, zoals al eerder bleek, wordt ook dat vooral in verband gebracht met de bedreigingen die voorkomen uit de ontwikkeling van informatietechnologie:

> 'De toenemende informatietechnologische mogelijkheden tot manipulatie van persoonsgegevens maken de positie van de burger steeds kwetsbaarder. Het is voor de individuele burger zeer moeilijk greep te houden op de wijze waarop er met zijn persoonsgegevens wordt omgegaan. Dat hangt samen met het feit dat de verwerking van persoonsgegevens zich in belangrijke mate aan zijn waarneming onttrekt. Deze achtergrond rechtvaardigt de instelling van een overheidsorgaan met eigen bevoegdheden om de naleving van de wettelijke voorschriften en de rechtsontwikkeling op dit punt te bevorderen.[136]

Een van de in de evaluaties van de WPR gesignaleerde problemen betrof het beperkte maatschappelijk draagvlak van de toezichthouder. In dat verband werd ook aangegeven dat de ontwikkeling van het privacyrecht zich tot dan in relatief isolement heeft voltrokken, en dat de toezichthouder maar in beperkte mate in maatschappelijke discussies was betrokken. Om dit probleem op te lossen voorziet de Wbp in extra bevoegdheden voor de toezichthouder en in de mogelijkheid van rechterlijke toetsing op het gebruik van de-

---

[134] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 134.
[135] Zie par. 4.5 en 4.8 van dit rapport; *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 132-133.
[136] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 26.

ze bevoegdheden. Verder wordt veel verwacht van de interactie tussen de toezichthouder en de functionarissen voor de gegevensbescherming in de verschillende bedrijven en sectoren.

> 'de ontwikkeling van het privacyrecht tot dusver [heeft] zich in relatief isolement heeft voltrokken. Daarmee is ook de Registratiekamer slechts in beperkte mate in maatschappelijke discussies betrokken. De verschillende in het onderhavige wetsvoorstel opgenomen extra bevoegdheden van de kamer, alsmede de mogelijkheid van rechterlijke toetsing op het gebruik daarvan, zullen het draagvlak van de rechtsvorming op dit gebied naar onze verwachting vergroten. Ook de interactie tussen de Registratiekamer en de eigen toezichthouders in verschillende bedrijven en branches, zal naar onze verwachting een verbreding van de groep van betrokken personen bij de rechtsontwikkelingen op dit gebied tot gevolg hebben.[137]

Om het maatschappelijk draagvlak van het Cbp verder te verbreden is verder bij amendement voorzien in een Raad van Advies. In deze raad nemen vertegenwoordigers zitting die vanuit verschillende geledingen van de samenleving te maken hebben met gegevensverwerkingen. Met deze raad, waarvan de leden dus gezamenlijk een zo representatief mogelijke afspiegeling moeten zijn van de maatschappij, wordt beoogd dat:

> 'het College voor wat betreft haar standpuntvorming over algemene aspecten van de bescherming van persoonsgegevens een sterker contact [krijgt] met de opvattingen van de samenleving hierover'.[138]

De Wbp beoogt het maatschappelijk draagvlak van de toezichthouder te verbreden en deze meer te betrekken in discussies over privacybescherming door te voorzien in extra bevoegdheden voor het Cbp, door rechterlijke toetsing van het gebruik daarvan mogelijk te maken, door instelling van een Raad van Advies en door interactie tussen de toezichthouder en de functionaris voor de gegevensbescherming.

De richtlijn verlangt in artikel 28, eerste lid, dat de toezichthouder in volledige onafhankelijkheid zijn taken moet kunnen vervullen. In de MvT wordt dit in verband gebracht met het toezicht dat de toezichthouder ook moet kunnen uitoefenen op gegevensverwerkingen in de overheidssector:

> 'De bevoegdheden van de [Registratie]Kamer richten zich in eerste aanleg, uitgaande van de verticale werking van het grondrecht op bescherming van de persoonlijke levenssfeer, tot de gegevensverwerkingen binnen de overheidssector. Deze positie vraagt om een onafhankelijk functioneren van de Kamer ten opzichte van die overheid.'[139]

Om deze reden heeft de wetgever ervoor gekozen om de toezichthouder, het Cbp, als zelfstandig bestuursorgaan (zbo) vorm te geven. Daarmee wordt het volgens de MvT mogelijk gemaakt dat het Cbp bij toezichthoudende en handhavende taken volledig vrij is in de prioriteitstelling. Verder zijn met het oog op de onafhankelijkheid van de toezichthouder in de wet specifieke regels opgenomen met betrekking tot de rechtspositie van de collegeleden van het Cbp.

Een en ander wordt in de loop van de parlementaire behandeling van de wet evenwel stukje bij beetje bijgesteld. Zo is de minister op grond van artikel 53, vierde lid, bevoegd het bestuursreglement van het Cbp goed te keuren. Met het oog op een goede en zorgvuldige uitoefening van zijn taken is bij een nota van wijziging vastgelegd dat in dit goed te keuren bestuursreglement ook regels worden gesteld omtrent de

---

137 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 41.
138 *Kamerstukken II* 1997-1998, 25 892, nr. 30; zie ook *Handelingen I* 3 juli 2000, p. 34-1625.
139 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 27.

werkwijzen en procedures van de toezichthouder.[140] Uit de parlementaire geschiedenis blijkt dat de minister deze bevoegdheid ziet als een instrument ter voorkoming van met name de risico's van belangenverstening door de veelheid van taken en bevoegdheden van de toezichthouder te voorkomen.[141]

Door het Cbp de status van een zbo te geven en in de Wbp de rechtspositie van de collegeleden vast te leggen beoogt de wetgever de onafhankelijkheid van de toezichthouder te waarborgen. De wet voorziet in een goedkeuringsbevoegdheid voor de minister met betrekking tot het Cbp-bestuursreglement, waarin ook regels worden gesteld omtrent de werkwijzen en procedures van de toezichthouder. Daarmee beoogt de wet belangenverstrengeling bij de toezichthouder te voorkomen.

Effectieve handhaving en versterken positie van verantwoordelijken tegenover Cbp

Om de toezichthouder in staat te stellen de wet op een effectieve wijze te handhaven voorziet de wet in een aantal nieuwe bevoegdheden en dwangmiddelen. Anders dan onder de WPR maakt de Wbp het in artikel 66 mogelijk dat het Cbp een bestuurlijke boete kan opleggen in het geval er niet is voldaan aan de meldplicht – overigens nadat daarover bij het parlementaire behandeling de nodige discussie aan vooraf was gegaan.[142] Verder voorziet de wet in artikel 65 in het opleggen van bestuursdwang, alsmede in artikel 75 in strafrechtelijke sancties.[143] Tegen de beslissingen van de toezichthouder over deze bevoegdheden staat beroep open bij de bestuursrechter. Daarmee wordt de rechtspositie van de verantwoordelijke versterkt. Ook daarmee wordt de regeling beter ingebed in het algemene recht.[144]

De Wbp beoogt het Cbp in staat te stellen de wet effectief te handhaven en voorziet daartoe in door de toezichthouder op te leggen bestuurlijke boetes en bestuursdwang, alsmede in enige strafrechtelijke sancties.

Rechtsbescherming

Waar het gaat om de rechtsbescherming van betrokkenen met betrekking tot de door de Wbp te bieden bescherming heeft de wetgever zoveel mogelijk willen aansluiten bij het algemene, dus niet privacyspecifieke recht – dit om te zorgen voor een betere inbedding in het rechtsstelsel.[145] Dit betekent dat de bestuursrechter bevoegd is ten aanzien van verwerkingen binnen de publieke sector en de civiele rechter voor verwerkingen in de private sector. Maar tot grote materiële verschillen in rechtsbescherming behoeft dat volgens de MvT niet te leiden. Voor zover er verschillen zijn wordt verwacht dat deze 'hun gerechtvaardigde oorsprong vinden in de aard van de rechtsverhouding'. Verder zijn de verschillen naar verwachting vooral van procedurele aard, aangezien deze het gevolg zijn van het bestaande systeem van rechtspleging dat uitgaat van verschillende procedures voor de burgerlijke rechter en de bestuursrechter.[146]

Waar het gaat om de rechtsbescherming van de verantwoordelijke tegenover het Cbp is, zoals gezegd, de positie van de verantwoordelijke versterkt.

---

[140] *Kamerstukken II* 1997-1998, 25 892, nr. 6, p. 21-22 en *Kamerstukken II* 1997-1998, 25 892, nr. 7, p. 10; *Kamerstukken II* 1997-1998, 25 892, nr. 8, p. 10 en 31; *Kamerstukken II* 1997-1998, 25 892, nr. 13, p. 14; vgl. *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 181.
[141] *Handelingen I* 3 juli 2000, p. 34-1630 en 1635, alsmede 1608; zie ook *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 27-28.
[142] *Kamerstukken II* 1998-1999, 25 892, nr. 8, p. 6.
[143] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 30, 186-188.
[144] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 26.
[145] Zie par. 3.3.1 en 3.3.5 van dit rapport.
[146] *Kamerstukken II* 1997-1998, 25 892, nr. 6, p. 20; *Kamerstukken II* 1998-1999, 25 892, nr. 11, p. 10.

Om te zorgen voor een betere inbedding van de wet in het rechtsstelsel beoogt de Wbp bij de rechtsbescherming van betrokkenen zoveel mogelijk aan te sluiten bij het algemene recht. De wet beoogt uitdrukkelijk de positie van de verantwoordelijken tegenover het Cbp te versterken.

3.3.6 Internationale gegevensdoorgifte

Waar het gaat om de doorgifte van persoonsgegevens naar derde landen laat de richtlijn weinig ruimte voor de nationale wetgever om een eigen invulling te geven. In de MvT wordt weer een relatie gelegd met informatiechnologische ontwikkelingen. De de bedoelingen van de doorgifteregels worden op de volgende wijze verwoord:

> 'De Unie is geen eiland in de wereld. Moderne informatietechnologische middelen maken de plaatsbepaling van gegevens steeds abstracter. Enerzijds werkt dit de mogelijkheden tot misbruik in de hand. De regelgeving dient handvatten te bieden hiertegen te kunnen optreden. Anderzijds kan het verkeer van persoonsgegevens in contacten met landen buiten de Unie niet aan zodanige beperkingen worden onderworpen dat daardoor bij voorbeeld het reguliere handelsverkeer onnodig zou worden belemmerd. De vastgestelde bepalingen beogen deze belangentegenstelling in evenwicht te brengen, althans het instrumentarium aan te reiken om dit in voorkomend geval te bewerkstelligen'.[147]

De wet beoogt te voorzien in een instrumentarium waarmee kan worden bewerkstelligd dat het reguliere handelsverkeer niet onnodig wordt belemmerd terwijl tegelijkertijd wordt voorkomen dat wet wordt omzeild of ontdoken door gegevens in derde landen te doen verwerken.

Als de desbetreffende gegevensverwerking wordt gemeld – en dat zal bij doorgifte als snel het geval zijn omdat er dan veelal niet meer sprake is van een vrijgestelde verwerking[148]– moet ook de doorgifte in de melding worden opgenomen. De reden daarvoor ligt volgens de MvT in het kunnen voldoen aan de op de lidstaten en de Commissie rustende verplichting van artikel 26, derde lid, richtlijn om elkaar op de hoogte te brengen van de gevallen waarin, naar hun oordeel, een derde land geen waarborgen voor een passend beschermingsniveau biedt:

> 'Om te kunnen voldoen aan artikel 25, derde lid, van de richtlijn is het nodig zicht te krijgen op deze verstrekkingen teneinde de regering in staat te stellen de Europese Commissie te verwittigen van gevallen waarin geen passend niveau van bescherming in het derde land aanwezig wordt geacht. Het maakt a contrario duidelijk dat het gegevensverkeer met landen binnen de Unie niet aan een dergelijk bijzonder toezicht is onderworpen'.[149]

Er is verder gekozen om in voorkomende gevallen een vergunningsvereiste te stellen aan gegevensdoorgiften naar derde landen. Uit de MvT blijkt dat met deze vergunning wordt beoogd een mogelijkheid ('noodklep') te bieden voor de gevallen waarin geen gebruik kan worden gemaakt van de wettelijke uitzonderingen:

> 'Deze bepaling bevat een noodklep indien de toegestane uitzonderingsgronden ontoereikend blijken. De Minister van Justitie kan in dat geval vergunning voor doorgifte verlenen. Aan de vergunning dienen nadere voorschriften te worden verbonden ter bescherming van de persoonlijke levenssfeer of de fundamentele rechten en vrijheden van per-

147 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 192.
148 Zie art. 44 Vrijstellingsbesluit.
149 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 137.

sonen. Deze voorschriften kunnen betrekking hebben op contractuele bepalingen die de verantwoordelijke in een overeenkomst met degene aan wie de gegevens worden doorgegeven, opneemt'.[150]

Daaruit kan worden opgemaakt dat de doorgiftevergunning is bedoeld voor betrekkelijk uitzonderlijke situaties. Als zodanig wordt dit vergunningvereiste in veel lidstaten niet gesteld.[151]

De wet voorziet bij wijze van 'noodklep' in de mogelijkheid van een doorgiftevergunning. Daarmee wordt beoogd doorgifte mogelijk te maken als er geen beroep kan worden gedaan op de wettelijke uitzonderingen op het doorgifte verbod.

3.4 Uitvoeringskosten

Over de kosten die zijn gemoeid met de uitvoering en naleving van privacywetgeving is in de parlementaire geschiedenis veel gezegd. In reactie daarop wijst de MvT vooral op de vrijstelling van de meldplicht, die wordt geregeld in het al eerder genoemde Vrijstellingsbesluit.[152] Daarover wordt opgemerkt dat het de bedoeling is een groot deel van de vele vormen van gegevensverwerking vrij te stellen.

> '[het] in de bedoeling ligt van deze vrijstellingsmogelijkheid op ruime schaal gebruik te maken. [153]

Ook wordt een aanmerkelijke lastenverlichting verwacht doordat de meldingsplicht voor handmatige bestanden, waar de WPR nog in voorzag, wordt geschrapt. Verder wordt erop gewezen dat de wet aansluit bij de realiteit van multifunctionele informatiesystemen en het mogelijk maakt om meerdere, uiteenlopende doeleinden van de gegevensverwerking vast te stellen.[154] Ook wordt ernaar gestreefd de nakoming van de aanmeldingsplicht zo eenvoudig mogelijk te maken, aangezien de daadwerkelijke naleving ervan is gebaat bij 'een zo min mogelijke administratieve belasting'.[155] In de parlementaire geschiedenis wordt daartoe genoemd de ontwikkeling van een diskette, te downloaden van de website van de toezichthouder, waarmee het meldproces op efficiënte wijze kan worden ondersteund.[156] De Wbp beoogt dat er op ruime schaal gebruik kan worden gemaakt van de vrijstellingen op de meldingsplicht. Waar meldingen vereist zijn wordt gestreefd naar het zo eenvoudig mogelijk maken daarvan, onder andere door middel van een meldingsdiskette. Een andere wijze waarop de wetgever beoogt de meldplicht eenvoudiger en gemakkelijker uitvoerbaar te maken is de mogelijkheid om meldingen te doen bij de FG:

> 'Wat betreft de procedure is er verder de mogelijkheid om in plaats van aan de Registratiekamer te melden bij een eigen toezichthouder met een op het eigen bedrijf of de eigen branche toegesneden aanmeldingsprocedure. Beide aspecten, inhoud en procedure, kunnen leiden tot besparingen ten opzichte van nu'.[157]

De Wbp beoogt problemen en kosten verband houdend met de meldplicht en de naleving daarvan te voorkomen onder andere door ook melding bij de FG mogelijk te maken en door de meldingsprocedure bij het Cbp te vereenvoudigen.

---

[150] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 195.
[151] Vgl. Economic Evaluation of the Data Protection Directive (95/46/EC), mei 2005.
[152] *Stb.* 2004, 261.
[153] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 140.
[154] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 34.
[155] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 139.
[156] *Kamerstukken I* 1999-2000, 25 892, nr. 92c, p. 21.
[157] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 34 en ook p. 39.

3.5 Technologie-onafhankelijkheid

De periode waarin de WPR tot stand is gekomen, kenmerkte zich door 'technologische turbulentie', een term die geïntroduceerd is in de Nota Wetgeving op de elektronische snelweg[158] uit 1998, en die daarin als volgt wordt getypeerd:

> "Nieuwe informatietechnieken en -producten volgen elkaar in hoog tempo op, of convergeren tot nieuwe media. De ontwikkeling van de techniek, het maatschappelijk gebruik ervan en de sociale en juridische problemen die erdoor worden opgeroepen, zijn in hoge mate onvoorspelbaar en kennen een hoge omloopsnelheid."[159]

Vanwege deze onvoorspelbaarheid en de hoge omloopsnelheid stelt dezelfde nota als norm dat regelgeving technologie-onafhankelijk moet worden geformuleerd, onder meer in het daarin vervatte toetsingskader voor wetgeving.[160] Het hierbij genoemde voorbeeld stelt dat:

> '[...] alle regels over privacy worden opgenomen in een algemene privacywet en niet in verschillende op technologie gebaseerde sectorspecifieke wetten.'[161]

Ook de vervanging van het begrip 'persoonsregistratie' door het begrip 'gegevensverwerking' wordt in de MvT in verband gebracht met het streven naar technologie-onafhankelijke wetgeving:

> 'De ontwikkeling van de techniek verloopt evenwel onafhankelijk van de ontwikkeling van het recht en het vormt een uitdaging aan de rechtspraktijk nieuwe juridische begrippen te ontwikkelen, die tot op zekere hoogte technologie-neutraal zijn en daardoor minder snel verouderen ten gevolge van technische ontwikkelingen. Het begrip «persoonsregistratie» is een voorbeeld van een technologie-afhankelijk begrip en het onderhavige wetsvoorstel neemt dan ook het meer neutrale begrip «gegevensverwerking » als aangrijpingspunt. Met dit nieuwe begrip wordt aangesloten bij de realiteit van netwerkvorming waarin de computers van weleer vaak slechts een ondergeschikt knooppunt vormen.'[162]

In de MvT wordt de mogelijkheid van een technologie-onafhankelijke wet overigens wel gerelativeerd:

> "Volledig technologie-onafhankelijke wetgeving behoort niet tot de reële mogelijkheden. Het enige dat kan worden nagestreefd is zo technologie-onafhankelijk mogelijke regelgeving. [...] Er moet daarom een tussenweg worden bewandeld tussen twee met elkaar onverenigbare uitersten. Aan de ene kant staat het ideaal van regelgeving die helder en duidelijk is: met een nieuwe technologie gelden de volgende gedragsvoorschriften. Aan de andere kant het ideaal van technologie-onafhankelijke regelgeving, die echter in het duister tast omdat nog volstrekt onduidelijk is hoe de techniek zich zal ontwikkelen.[163]

De technologie-onafhankelijkheid wordt dus gerealiseerd door een middenweg te kiezen qua detaillering: de Wbp bevat vele open normen, en wordt aangevuld en gespecificeerd door aanvullingen in sectorale wetgeving, zoals de Wet Geneeskundige Behandelings Overeenkomst (WGBO) en de Archiefwet[164], en ook door de invulling die de rechtspraak geeft aan de open normen van de wet.[165]

---

158 *Kamerstukken II* 1997-1998, 25 880, nr. 2.
159 *Kamerstukken II* 1997-1998, 25 880, nr. 2, p. 4.
160 *Kamerstukken II* 1997-1998, 25 880, nr. 2, p. 14.
161 *Kamerstukken II* 1997-1998, 25 880, nr. 2, p. 14.
162 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 7.
163 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 7.
164 Zie sectorale hoofdstukken.
165 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 6.

De Wbp beoogt zo technologie-onafhankelijk mogelijke regelgeving. Daarbij beoogt de wet een aanvaardbaar evenwicht te vinden tussen enerzijds duidelijke en heldere regels en anderzijds technologie-onafhankelijke regelgeving die in een context van snelle technologische ontwikkelingen onzeker kan zijn.

3.6 Conclusies

Formele doelstellingen

De Wbp beoogt de richtlijn te implementeren en binnen de door de richtlijn gegevens bandbreedte gedeeltelijk nadere invulling te geven aan de voorwaarden waaronder verwerkingen rechtmatig zijn. De wet beoogt verder uitvoering te geven aan de opdracht van de grondwetgever om regels te stellen in verband met de vastlegging en verstrekking van persoonsgegevens, inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en het gebruik dat daarvan wordt gemaakt, en de verbetering daarvan. De Wbp beoogt daarnaast ook uitvoering te geven aan het Verdrag inzake gegevensbescherming en aan te sluiten bij de jurisprudentie van het EHRM over artikel 8 EVRM.

Werkingsfeer en toepassing

Voorzover mogelijk binnen de door de richtlijn gegeven ruimte beoogt de Wbp in beginsel niet minder bescherming te bieden dan de WPR. De Wbp beoogt dan ook zoveel mogelijk uit te gaan van het begrippenkader van de WPR, teneinde gebruik te kunnen maken van de in het kader van deze wet ontwikkelde jurisprudentie.

Om vragen over de verhouding tussen de Wbp en sectorale wetten te voorkomen gaat de wet uit van het uitgangspunt dat de wet van toepassing is, tenzij er in een sectorale wet anders is bepaald. Voor zover mogelijk beoogt de wet geen onderscheid te maken tussen verwerkingen die wél en verwerkingen die niet onder het gemeenschapsrecht vallen. De Wbp beoogt een evenwicht te bewerkstelligen tussen privacybescherming en andere grondrechten, meer in het bijzonder de vrijheid van meningsuiting. Daarbij beoogt de wet aan te sluiten bij de jurisprudentie hierover.

Normatieve kaders

De Wbp beoogt goed ingebed te zijn in het rechtsstelsel en beter (dan de WPR) aan te sluiten bij overige wetgeving. In verband daarmee beoogt de wet door middel van open en vage normen te voorzien in het instrumentarium voor de afweging van de bij gegevensverwerkingen betrokken belangen. De Wbp beoogt daartoe de positie van de betrokkenen te versterken door onduidelijkheden over het verantwoordelijkebegrip op te helderen door middel van het aansluiten bij bestaande privaatrechtelijke en publiekrechtelijke verhoudingen. Ook beoogt de De Wbp beoogt waar mogelijk aan te sluiten bij potentiële risico's van gegevensverwerkingen. In aanvulling op de bescherming van privacy-grondrechten beoogt de Wbp waarborgen te bieden tegen verwerkingen van persoonsgegevens die afbreuk kunnen doen aan de werking van andere grondrechten, met name die betrekking hebben op de handelingsvrijheid van individuen en de toegang tot de rechter.

Transparantie

Om de positie van betrokkenen tegenover verantwoordelijken te versterken beoogt de Wbp de transparantie van gegevensverwerkingen te vergroten. De wet doet dit door rechten toe te kennen aan betrokkenen en daarmee corresponderende verplichtingen op te leggen aan verantwoordelijken, alsmede door het instellen van een toezichthouder..

Zelfregulering

De Wbp beoogt dat de materiële normen via zelfregulering (gedragscodes, FG en meldingen) nader worden ingevuld. Zodoende beoogt de wet het mogelijk te maken dat wordt gedifferentieerd naar de context waarin de werkingen plaatsvinden. De Wbp beoogt de opstelling van gedragscodes te bevorderen door de procedure te versimpelen (en bestaande inspraakmogelijkheden te schrappen). Verder beoogt de wet de positie van verantwoordelijken ten opzichte van het Cbp op te helderen door beroep bij de bestuursrechter open te stellen tegen beslissingen inzake de goedkeuring van gedragscodes. De Wbp beoogt door het instituut van de FG te komen tot een betere, meer omvattende invulling van de eigen verantwoordelijkheid van verantwoordelijken. Het maakt maatwerk mogelijk en wordt geacht de kennisontwikkeling over gegevensbescherming en privacybewustzijn te bevorderen.

Ook de meldplicht kan worden gezien als een middel om zelfregulering, namelijk als op het niveau van de verantwoordelijke. Met de melding beoogt de Wbp de verantwoordelijken in staat te stellen aan te sluiten bij hun eigen specifieke behoeften.

Toezicht en rechtsbescherming

De Wbp beoogt het maatschappelijk draagvlak van de toezichthouder te verbreden en deze meer te betrekken in discussies over privacybescherming door te voorzien in extra bevoegdheden voor het Cbp, door rechterlijke toetsing van het gebruik daarvan mogelijk te maken, en door instelling van een Raad van Advies.

De Wbp beoogt het Cbp in staat te stellen de wet effectief te handhaven en voorziet daartoe in een bestuurlijke boete en bestuursdwang. Om te zorgen voor een betere inbedding van de wet in het rechtsstelsel beoogt de Wbp bij de rechtsbescherming van betrokkenen zoveel mogelijk aan te sluiten bij het algemene recht. De wet beoogt uitdrukkelijk de positie van de verantwoordelijken tegenover het Cbp te versterken.

Internationale gegevensdoorgifte

De wet beoogt te voorzien in een instrumentarium waarmee kan worden bewerkstelligd dat het reguliere handelsverkeer niet onnodig wordt belemmerd terwijl tegelijkertijd wordt voorkomen dat wet wordt omzeild of ontdoken door gegevens in derde landen te doen verwerken. De wet voorziet bij wijze van 'noodklep' in de mogelijkheid van een doorgiftevergunning. Daarmee wordt beoogd doorgifte mogelijk te maken als er geen beroep kan worden gedaan op de wettelijke uitzonderingen op het doorgifte verbod.

Uitvoeringskosten

De Wbp beoogt problemen en kosten verband houdend met de meldplicht en de naleving daarvan te voorkomen onder andere door ook melding bij de FG mogelijk te maken en door de meldingsprocedure bij het Cbp te vereenvoudigen.

Technologie-onafhankelijkheid

De Wbp beoogt zo technologie-onafhankelijk mogelijke regelgeving. Daarbij beoogt de wet een aanvaardbaar evenwicht te vinden tussen enerzijds duidelijke en heldere regels en anderzijds technologie-onafhankelijke regelgeving die in een context van snelle technologische ontwikkelingen onzeker kan zijn.

Hoofdstuk 4: Algemene knelpunten

4.1 Inleiding

Dit hoofdstuk is het eerste van vier hoofdstukken waarin wordt nagegaan welke knelpunten er in literatuur en rechtspraak worden geïdentificeerd bij de toepassing van de wet, alsmede welke oplossingsrichtingen worden gesuggereerd. In dit hoofdstuk wordt gekeken naar de algemene, sectoroverschrijdende knelpunten. In de drie daaropvolgende hoofdstukken wordt vervolgens bezien welke knelpunten er in de literatuur zijn geïdentificeerd met betrekking tot de particuliere, publieke en semi-publieke sector.

Zoals uiteengezet in het inleidende hoofdstuk wordt in dit onderdeel van de literatuurstudie uitgegaan van de onderscheiden zes thema's van de wet, te weten: werkingssfeer en toepassing, normatieve kaders, zelfregulering, transparantie en rechten van betrokkenen, rechtsbescherming en toezicht, en internationale gegevensdoorgifte. Aansluitend wordt ingegaan op de overige in het voorgaande geïdentificeerde thema's of aspecten, te weten die betrekking hebben op de uitvoeringskosten en de technologie-onafhankelijkheid.

4.2 Werkingssfeer en toepassing

4.2.1 Begrippen

Over de begrippen 'persoonsgegevens' en 'bestand' werd al ten tijde van de WPR en zelfs daarvoor al het nodige geschreven.[166] Omdat de in deze wet gegeven omschrijvingen van de begrippen inhoudelijk aansluiten bij die van de Wbp[167] is deze literatuur ook relevant voor de laatste wet. Veel kritiek is er op de onduidelijkheid en onbepaaldheid of algemeenheid en alomvattendheid van de begrippen, die ook in de lagere regelgeving niet voldoende nader worden gepreciseerd. Het meest principieel zijn De Hert & Gutwirth.[168] Hoewel deze auteurs niet negatief zijn over adequaatheid van de privacywetgeving ligt voor hen het 'echte probleem' van de privacy-richtlijn, en dus ook de Wbp, met name in het te algemene en daardoor te weinig onderscheid makende karakter van de regelgeving:

> 'In het streven naar algemeenheid gaat [de wetgeving gericht op] data protection voorbij aan de noodzaak te discrimineren en te begrenzen. Alles is een 'verwerking' wat wil zeggen dat het aanleggen van een adresbestand en het maken van een profiel [bijv. t.b.v. terreurbestrijding] dezelfde status krijgt. Alles is een 'persoonsgegeven' wat maakt dat een foto van een persoon (erg veelzeggend en voldoende voor velen om een oordeel op te baseren) dezelfde waarde krijgt toegemeten als een stukje tekst over diezelfde persoon. De macht wordt op deze wijze niet ernstig genomen. Hier past geen formele benadering maar is meer nodig'.

De overige kritiek heeft veelal een meer praktische achtergrond en betreft de werkbaarheid of onwerkbaarheid van de wettelijke begrippen. Soms betreft dergelijke kritiek een enkele terloopse opmerking die wordt gemaakt in een ander verband, maar wel aansluit bij de kritiek van De Hert & Gutwirth. Zo merkt Kroes[169] op dat de reikwijdte van de Wbp wellicht te ruim is omdat daaronder ook gegevens vallen waarbij de privacy niet of nauwelijks in het geding is, zoals een visitekaartje of een professioneel e-mailadres. Cuij-

---

166 Bijv. De Graaf 1987.
167 *Kamerstukken II* 1997-1998, 25 892 nr. 3, p. 45 resp. 53.
168 De Hert & Gutwirth 2004, p. 587-631.
169 Kroes 2003, p. 24.

pers[170] en de Raad van de Centrale Ondernemingsorganisaties (RCO)[171] wijzen met meer nadruk op dit punt, de laatste met name waar het gaat om foto's:

> 'not all images, such as photographs, necessarily always contain personal data. Article 3(1) implies that the Directive covers practically any processing of personal data. This would also include all sorts of relatively trivial cases, which in turn would imply that the persons concerned could invoke their rights to provision of information and inspection etc.'

In het verlengde van het voorgaande stelt het RCO de vraag of het begrip niet veel te veel activiteiten, en dan met name betrekkelijk risicoloze 'technische' verwerkingen, onder de privacywetgeving vallen:

> 'Activities such as collecting and using personal data and the transfer of the right to use personal data can have consequences for the individuals concerned. Other activities are subsidiary to these and should rather be permitted by definition if the above-mentioned activities are permitted. One might wonder therefore whether any simple activity involving personal data constitutes "processing" that must be regulated under the Directive. In the case of electronic communication, for example, data are often (technically) stored by an intermediate person or service provider. The advantages of branding this "processing" – with the result that all activities involving the data come fall within the scope of the Directive – are not clear.'

Al voor de inwerkingtreding van de wet wees Berkvens[172] op de problemen die voortkomen uit het dynamische en soms 'tweekoppige karakter' van de verschillende wettelijke begrippen. Onder andere naar aanleiding van deze kritiek heeft Holvast[173] nader onderzoek gedaan naar deze begrippen. Deze auteur wijst op de onduidelijkheid die het gevolg is van het herleidbaarheids- of identificeerbaarheidscriterium. Aan de hand daarvan wordt bepaald of er sprake is van een persoonsgegeven in de zin van de wet. Of er sprake is van herleidbaarheid is afhankelijk van zowel direct als indirect identificerende gegevens, waardoor het kan afhangen van toevallige factoren en omstandigheden of iets als persoonsgegeven heeft te gelden. Verder wijst hij erop dat het herleidbaarheidscriterium onduidelijk kan zijn doordat het contextafhankelijkheid is: wat voor de ene persoon of organisatie een persoonsgegeven is hoeft dat voor de andere niet te zijn. Ook wijst hij erop dat onduidelijk is over hoeveel personen er gegevens moeten zijn opgenomen om te kunnen spreken van een 'persoonsregistratie' in de zin van de WPR, welk begrip zoals gezegd overeenkomt met dat van een 'bestand' in de Wbp.

Cuijpers[174] stelt dat de onduidelijkheid over de begrippen 'verantwoordelijke', 'bewerker' en 'derde' en de onderlinge verhouding van deze begrippen vooral bij fusies en overnames, en in concernverband aanleiding geven tot problemen en knelpunten. Deze auteur lijkt daarbij vooral te denken aan problemen in de private sector. In de bijeenkomst met domeindeskundigen in het kader van dit onderzoek werd dit evenwel ook genoemd als probleem bij fusies van scholen of zorginstelling, alsmede in allerlei samenwerkingsverbanden. Als oplossing wordt wel voorgesteld dat gebruik wordt gemaakt van het in Duitsland veel bediscussieerde, maar niet ingevoerde concept van zgn. 'Konzern Privileg', dat wil zeggen dat persoonsgegevens binnen één concern worden verwerkt als ware het binnen één en dezelfde verantwoordelijke.[175] Meer daarover in hoofdstuk 5.

Ook technologische ontwikkelingen worden gezien als een factor die bijdraagt aan de onduidelijkheid van de wettelijke begrippen. In een onderzoek over de toepassing van privacyregels op internetberichten komt

---

[170] Cuijpers 2006, p. 12; zie hierover ook het Advies van de Raad van State over het voorstel van wet, *kamerstukken II* 1997–1998, 25 892, A, p. 4-5.
[171] RCO 2003; zie voor de discussie over foto's en beelden ook het Implementatierapport, p. 20-21.
[172] Zie o.a. Berkvens 1992, p. 41-54; Berkvens 1994, p. 151-175.
[173] Holvast 1999, p. 201-204; Holvast 1996, p. 84-85.
[174] Cuijpers 2006, p. 12.
[175] Dit bleek uit de interviews die voorafgaand aan het onderhavige onderzoek zijn gehouden.

Nouwt[176] tot de 'voorzichtige conclusie' dat de definities van de actoren van de wet (dus verantwoordelijke, bewerker, betrokkene enz.) moeilijker hanteerbaar worden als gevolg van het diffuser worden van de technische werkelijkheid. Veel meer uitgesproken daarover is Berkvens.[177] Deze auteur stelt vast dat de wettelijke definities een ruime bandbreedte hebben waarvan niet duidelijk is hoe deze gehanteerd gaat worden. Als gevolg daarvan is volgens hem niet alleen de rechtszekerheid in het geding maar kan de wetgeving een serieuze bedreiging gaan vormen voor de ongestoorde invoering van nuttige technologie. Dit omdat:

> '[d]e werkelijkheid van de eenentwintigste eeuw [...] zich niet [laat] meer in het begrippenapparaat uit 1980 laat persen'

In een latere studie is Holvast[178] daarover genuanceerder maar toch kritisch. In zijn studie over de toepassing van privacywetgeving op de geautomatiseerde, gestructureerde en genormeerde berichtenuitwisseling[179] stelt hij vast dat er kennelijk discrepanties bestaat bestaan tussen theorie en praktijk. Maar deze zijn volgens hem oplosbaar en zijn niet van dien aard dat de rechtzekerheid in het geding is. Wel dringt hij erop aan dat 'matigheid' wordt betracht bij de interpretatie van de begrippen. Dit om te voorkomen dat alle gegevens onder het persoonsgegevensbegrip vallen, waardoor de naleving van de wet ernstig wordt belemmerd omdat, de wet dan overal op van toepassing is. Uit het Implementatierapport blijkt dat dergelijke voorstellen ook worden gedaan door uiteenlopende andere organisaties. Zo dringen het European Privacy Officers Forum (EPOF) en de Federatie van Europese Direct Marketing (FEDMA) op een meer 'reasonable and flexible interpretation' van de wettelijke begrippen – naar mag worden aangenomen wordt daarmee (ook) gedoeld op een interpretatie die een minder verstrekkende, dus beperktere reikwijdte van deze kernbegrippen betekent.[180]

In verband met het voorgaande is van belang dat de Artikel 29 Werkgroep naar aanleiding van het Implementatierapport van de Europese Commissie onlangs heeft aangekondigd zich te gaan inspannen om een bijdrage te leveren aan een uniforme, geharmoniseerde interpretatie van de belangrijkste begrippen uit de richtlijn.[181] Aangenomen mag worden dat deze inspanningen ook zullen zijn gericht op het verduidelijken van de begrippen en deze beter hanteerbaar te maken. In hoeverre dat leidt tot begrippen met een beperktere reikwijdte is evenwel niet te zeggen. Uit enkele van haar publicaties, zoals die over cookies, RFID en locatiegegevens, blijkt dat de werkgroep in het verleden juist de grenzen van de wettelijke begrippen leek te willen oprekken.[182]

Terstegge[183] is uitgesproken over de technologische ontwikkeling en de onhoudbaarheid van de begrippen in de Wbp. Hij plaatst vraagtekens bij de technologie-onafhankelijkheid van deze begrippen en merkt op dat deze onder druk komen te staan door de invoering van met name RFID[184]-toepassingen en concepten als 'ubiquitous computing' of 'ambient intelligence'. Hij meent dat dergelijke ontwikkelingen het einde zullen gaan betekenen van de privacywetgeving zoals wij die nu kennen. De nieuwe wetgeving zal volgens deze auteur meer moeten uitgaan van 'privacy-by-design' en niet gericht moeten zijn op het gebruik van

---

[176] Nouwt 1999, p. 89-90.
[177] Berkvens 1994, p. 151-175.
[178] Holvast 1999, p. 201-204.
[179] Zgn. electronic data interchange ofwel 'EDI'.
[180] Implementatierapport, p. 15.
[181] Art. 29 Werkgroep 2006a; zie voor een toelichting Kohnstamm & Fontein 2006, p. 127-128.
[182] Art. 29 Werkgroep 2002; Art. 29 Werkgroep 2005a; zie ook bijv. Art. 29 Werkgroep 2005c.
[183] Terstegge 2005, p. 39-40.
[184] Radio Fequency Identification, d.w.z. de technologie waarmee met behulp van radiosignalen de unieke identificatie van producten, dieren en personen op afstand mogelijk wordt gemaakt; zie over RFID, 'ubiqituous computing' en 'ambient intelligence', Schermer 2005, p. 15-22.

gegevens maar het misbruik daarvan. Dat laatste wordt ook door Berkvens[185] betoogd. Deze auteur verwijst in dat kader naar een in opdracht van de Zweedse regering verrichte studie uit 1998.[186]

In meer algemene termen wijzen verschillende andere auteurs op de problemen die voortkomen uit de onbepaaldheid van de wettelijke begripsomschrijvingen. Van der Horst[187] wijst erop dat de wet door de gehanteerde definities een enorme reikwijdte heeft, wat naleving en de handhaving daarvan problematisch maakt. Waar het gaat over de in de wet en de richtlijn gebruikte begrippen spreekt Berkvens[188] van een 'teveel aan interpretatieruimte', waarmee de rechtszekerheid niet is gediend. En ook wijst hij erop dat deze situatie minder gewenst is omdat de wet strafrechtelijke consequenties verbindt aan een aantal verwerkingen die niet in overeenstemming met de wet zijn gedaan, terwijl er ook vragen ontstaan over de reikwijdte van de informatieplicht of kennisnemingrechten.[189] Holvast[190] is optimistischer over de te grote reikwijdte van de wettelijke begrippen, maar verwacht wel dat er moet worden gezocht naar 'creatieve oplossingen'.

Nog voor de implementatie van de richtlijn pleitte Verhey voor terughoudendheid met precisering van de normen uit de richtlijn in de Wbp:

> 'Precisering van normen die in zeer uiteenlopende casusposities moeten worden toegepast, kan tot gevolg hebben dat de wet een keurslijf wordt dat onvoldoende op de praktijk is toegesneden. […] Voorkomen moet worden dat de wettelijke normen zo worden ingericht dat zij hetzij te weinig waarborgen bevatten voor de geregistreerde, hetzij te knellend zijn voor degenen die de persoonsgegevens verwerken. Te verregaande detaillering van de wet houdt bovendien het risico in […] dat de bandbreedte van de Richtlijn wordt overschreden'[191]

In het Implementatierapport onderschrijft de Commissie dat de ruime definities aanleiding geven tot problemen. Echter, omdat de richtlijn nadrukkelijk een hoog beschermingsniveau beoogt en omdat de richtlijn van toepassing is op een groot aantal sectoren en in veel uiteenlopende contexten geeft zij (vooralsnog) niet de voorkeur aan het nader specificeren van de begrippen:

> 'Some contributors to the review proposed the amendment of the Directive to add more detail or specification to achieve this convergence. The Commission prefers to proceed at least initially by other means. Furthermore, the general nature of this Directive, i.e. the fact that it applies to a large number of sectors and contexts, generally argues against adding more detail or specification.'[192]

Welke oplossingen de Commissie wel voorstaat is evenwel niet duidelijk. Hustinx[193] is geen voorstander van een hernieuwde discussie over de reikwijdte van de wettelijke begrippen. Dit omdat hij voorstander is van een brede werkingssfeer, en ook omdat de discussies over de reikwijdte van de begrippen volgens hem leiden tot dogmatische en praktische problemen. En daarbij ziet hij zo een discussie als een 'signaal van zwakte':

> '[een discussie over de reikwijdte van begrippen] is de weg terug, want daarmee bouw je een enorm dogmatisch en praktisch probleem aan de voordeur. Elke keer weer discussies over de vraag 'is dit nu wel of niet een persoonsgegeven'. Ik ben een groot voorstander

---

185 Berkvens 2004b, p. 269.
186 Swedish It Law Observatory, 1998.
187 Van der Horst 2002, p. 113.
188 Berkvens 1994, p. 151-175.
189 Berkvens 2005b, p. 258-259.
190 Holvast 2002b, p. 370.
191 Verhey 1997, p. 255.
192 Implementatierapport, p. 11.
193 Zie Prins 2003, p. 69-73.

van een brede werkingssfeer die je dan wel verstandig en flexibel moet toepassen. Door nu aan de richtlijn te morrelen geef je internationaal een signaal van zwakte af en ontstaat er wederom een discussie van jaren met de bijbehorende implementatietrajecten.'

Een ander geluid komt van Prins.[194] Zij vraagt zich af of het begrip persoonsgegevens als uitgangspunt van de wet überhaupt wel voldoende is om aan burgers de bescherming te bieden in een maatschappij waarin identificatie en 'identiteiten' centraal lijken te komen staan. Het gaat volgens haar in toenemende mate niet alleen om de vraag of persoonsgegevens mogen worden verwerkt, maar om de vraag hoe en in welke combinatie ze worden verwerkt. De vraag is dan of het begrippenapparaat van de Wbp daar voldoende op is toegesneden. Waar het gaat over RFID en biometrie stelt Nas[195] min of meer dezelfde vragen.

Een aantal auteurs ziet de onduidelijkheid en onbepaaldheid van de wettelijke begrippen als een knelpunt dat de naleving van de wet belemmert en in de weg kan staan aan technologische ontwikkeling en innovatie. Voorgestelde oplossingsrichtingen lopen uiteen van een terughoudende interpretatie en een verstandige flexibele toepassing tot een vergaande heroverweging van de wijze van regulering. Andere auteurs en de Commissie pleiten voor behoud van de brede werkingssfeer.

4.2.2 Reikwijdte en toepassing

Omnibuswetgeving: één wet voor alles

Er is betrekkelijk veel discussie over het algemene karakter van de regelgeving of ook wel de keuze voor een omnibuswet in plaats van meer specifieke wetgeving voor verschillende sectoren en verwerkingen. Voor een deel gaat het dan over de alomvattendheid van de begrippen van de wet en in verband daarmee ook over de algemene, onbeperkte gelding van de wet, waarop de in de vorige paragraaf van dit rapport is ingegaan. Daarnaast gaat het over de keuze van de wetgever om uit te gaan van een algemene wet die gelijkelijk van toepassing is op alle maatschappelijke sectoren. Eén wet voor alles, ofwel een 'omnibuswet'.

Verschillende auteurs zetten zich daartegen af. Blok[196] meent dat er goede argumenten zijn om te uit te gaan van een sectorale benadering, zoals die in de Verenigde Staten wordt gevolgd. In deze benadering kan de wetgeving veel meer worden toegespitst op de verwerkingen en risico's in specifieke sectoren. Maar dat betekent volgens deze auteur niet dat deze wetgeving daardoor te weinig bescherming biedt, zoals onder andere door wetgevers wel wordt aangenomen maar eigenlijk niet of nauwelijks door hen blijkt te kunnen worden onderbouwd.[197] Aan omnibuswetgeving zijn, zo geeft hij aan, een aantal principiële en praktische bezwaren verbonden. Allereerst noemt Blok het principiële bezwaar dat onze samenleving uitgaat van de idee dat personen in beginsel zelf in staat zijn om hun leven in te richten op basis van hun eigen opvattingen en dat de overheid alleen ingrijpt als dat nodig is om de vrijheid en gelijkheid van burgers te waarborgen. En daarmee verhoudt zich zelfregulering beter dan een regeling door de wetgever. Van praktische betekenis is dat zelfregulering beter kan aansluiten bij de praktijk van degenen die met de gegevens werken, terwijl ook de naleving beter is gewaarborgd als de regels zijn opgesteld door degenen die er mee te maken hebben en niet van bovenaf zijn opgelegd.

In dat verband wijst deze auteur erop dat zelfregulering flexibeler is dan wetgeving, en dus beter in staat is om technologische ontwikkelingen en innovaties bij te houden. In aanvulling daarop noemt Blok nog dat omnibuswetgeving, en met name de Wbp, uitermate ingewikkeld en onoverzichtelijk is en tendeert naar ineffectieve bureaucratische procedures. Omdat omnibuswetgeving per definitie erg abstract en algemeen

194 Prins 2004a, p. 34-47; Prins 2004b.
195 Nas 2005, p. 105-109.
196 Blok 2002, p. 304.
197 Vgl. Blok 2005b, p. 246-252.

moet zijn, moeten de materiële normen daarvan altijd worden ingevuld in bijzondere, sectorale wetten, besluiten en/of gedragscodes, zodat er eerder meer dan minder regels zijn waarmee verantwoordelijken en betrokkenen rekening moeten houden.[198] Dat laatste wordt onderschreven door Holvast[199] die in een kritische beschouwing over de Wbp stelt dat

> 'de privacy via andere [en] meer via sectorale wetgeving beschermd kan en moet worden, ook al zal daar de afweging steeds een politieke blijven.'

Berkvens[200] is op hoofdlijnen dezelfde mening toegedaan als Blok. In een korte beschouwing over de systematiek van de Wbp, door hem gedefinieerd als een 'publiekrechtelijk getinte gebruiksregulerende omnibus', stelt hij vast dat de keuze van de wetgever voor een 'alles-in-een-regeling' eigenlijk van begin af aan al is achterhaald door de feiten – enerzijds door een groot aantal afwijkende overheidsregelingen en anderzijds door het gegeven dat informatiebetrekkingen in de private sector ook nog eens vaak worden geregeld in afzonderlijke wetten, zoals de Telecommunicatiewet of de Wet Consumentenkrediet. Hij merkt op dat de praktijk behoefte heeft aan maatwerk en meent dat de wetgever:

> 'al in een vroeg stadium een voorbeeld had kunnen nemen aan de Amerikaanse benadering van maatwerkwetgeving per bestaand probleemgebied. Nu zitten wij in een verwarrend duaal systeem met enerzijds niet altijd relevante algemene regels en anderzijds integrale maatwerkbenaderingen.'

Uit zijn betoog blijkt dat Berkvens in verband hiermee vooral problemen ziet in de private sector. Echter, vergelijkbare geluiden zijn ook te horen als het gaat om de publieke en semi-publieke sector. Als oplossing voor deze problematiek maakt Berkvens zich met anderen[201] al jaren sterk voor het implementeren van de wet in het Burgerlijk Wetboek in plaats van de gevolgde omnibuswet-benadering van 'een-wet-voor-alles'. Cuijpers[202] heeft dit onderzocht en komt tot tot de conclusie dat haar onderzoek

> 'niet zodanige contra-indicaties heeft opgeleverd dat van implementatie in het Burgerlijk Wetboek moet worden afgezien'.

Verder geeft zij aan dat een aantal van de gesignaleerde knelpunten zou kunnen worden verholpen door de richtlijn in het Burgerlijk Wetboek te implementeren. Behalve dat dit alternatief voor de Wbp beter recht zou doen aan de belangen van betrokkenen en verantwoordelijken, en meer in het algemeen de onderliggende rechtsverhoudingen, maakt dit de regeling korter, eenvoudiger en beter kenbaar, alsmede flexibeler, aldus Cuijpers.

Hustinx[203] bestrijdt de kritiek van Berkvens en anderen en verwerpt de door Cuijpers onderzochte mogelijkheid van implementatie van de richtlijn in het Burgerlijk Wetboek. In het licht van de ontwikkeling van het privacybegrip vindt hij het begrijpelijk dat de bescherming van persoonsgegevens ruim wordt opgevat en niet beperkt blijft tot de gegevens die direct raken aan de persoonlijke levenssfeer van betrokkenen. Juist de onzekere reikwijdte van het privacybegrip heeft volgens deze auteur geleid tot de idee dat persoonsgegevens ook los van de privacy moeten worden beschermd. En daarbij meent hij dat er ook praktische overwegingen zijn om uit te gaan van wetgeving met een algemene strekking. Een ander aanpak leidt volgens hem tot:

> 'een versnipperde of verkokerde aanpak, met alle bijbehorende afbakeningsproblemen, lacunes en inconsistenties'

---

198 Blok 2005b, p. 246-252.
199 Holvast 2005b, p. 242-245.
200 Berkvens 2004b, p. 269.
201 Zie bijv. Berkvens 1983, p. 42-45; Berkvens & Van Esch 1994, p. 93-100; zie verder de gesprekken met zowel Hirsch Ballin, Berkvens en Holvast in Prins 2003, resp. p. 56-57, p. 60 en p. 67-68.
202 Cuijpers 2004, m.n. p. 375-382.
203 Hustinx 2004, p. 270-272.

De vraag welke belangen bij de verwerking van persoonsgegevens zijn betrokken is altijd mede afhankelijk van de context waarin de gegevens worden verkregen en vastgelegd. En dat betekent volgens Hustinx dat de wettelijke regels veel ruimte moeten bieden voor het maken van de noodzakelijke afwegingen. Ook wijst hij erop dat een overkoepelende omnibus-benadering het voordeel heeft dat de ontwikkelingen op dit gebied in hun onderlinge samenhang kunnen worden bezien. En dat heeft grote voordelen boven de in de Verenigde Staten gevolgde sectorale benadering, die volgens hem tot 'legendarische problemen' heeft geleid. Zo was wel de videoverhuurbranche gereguleerd maar niet medische gegevens in de zorgsector. Eerder, in een interview ter gelegenheid van de beëindiging van het onderzoeksprogramma IT en Recht, verwoordde Hustinx de voordelen van de omnibusbenadering als volgt:

> 'Natuurlijk zou je een heleboel regels van de Wbp kunnen verspijkeren in de Awb en het BW en ze kunnen voorzien van diverse strafsancties. Maar ik denk dat je dan de *pointe* net mist, namelijk juist de integrale aanpak en de verzekering dat een en ander ook daadwerkelijk wordt nageleefd. Zowel het bestuursrecht als het burgerlijk recht leggen in wezen voortdurend de nadruk op het initiatief van de belanghebbende. Het gehele procesrisico ligt dus bij de individuele burger en uiteindelijk is de gehele samenleving er niet mee gediend als de handhaving niet wordt geactiveerd. De bescherming van persoonsgegevens heeft ook een publieke dimensie, hetgeen betekent dat er in het algemeen gesproken verkeersregels moeten zijn om dit belang te beschermen'.[204]

De omstandigheid dat op deelgebieden in aanvulling op de Wbp nog andere, al dan niet sectorale wetten van toepassing kunnen zijn, ziet Hustinx[205] niet als een probleem. Het gebruik van schakel- en verwijsbepalingen kan er naar volgens hem voor zorgen dat de relevante juridische omgeving in de toepassing daarvan wordt betrokken. Hetzelfde geldt voor de zelfregulering, meent hij.

Gutwirth & De Hert[206] stellen met enige nadruk dat de wetgever duidelijke keuzes moet maken en de onbepaaldheid en onbegrensdheid van de wet nader moet invullen, bijvoorbeeld als het gaat om de controle van e-mailverkeer van werknemers door werkgevers. En dat zou dan bijvoorbeeld kunnen in het arbeids- of privaatrecht.

In de praktijk lijkt er evenwel maar weinig draagvlak te zijn voor een sectorale benadering of een andere dan een omnibusbenadering. Hoewel het te algemene karakter van de wet werd gezien als een van de belangrijkste knelpunten van de wet, bestaat de vrees dat zo een sectorale benadering aanleiding geeft tot nog meer regels en een ingewikkelder, minder overzichtelijke regime.[207]

Volgens sommige auteurs leidt het algemene, omnibuskarakter van de wet tot grote knelpunten, waarvan de ingewikkeldheid en de inflexibiliteit het meest in het oog springen. Een enkele andere auteur meent dat een omnibus noodzakelijk is om alle betrokken belangen in hun onderlinge samenhang te kunnen bezien. Vanuit de praktijk wordt aangegeven dat er vrijwel geen behoefte is aan sectorale wetgeving in plaats van de Wbp.

Territoriale toepassing: op wie en op wat is de wet van toepassing

Over de toepassing van de wet maakt de Commissie in het Implementatierapport een paar opmerkingen die duiden op knelpunten waar organisaties mee te maken hebben die vestigingen hebben in meerdere lidstaten. In de consultatie die voorafging aan het rapport is vanuit verschillende kanten kritiek geuit op het gegeven dat volgens de toepassingsregels van artikel 4 van de richtlijn dergelijke lidstaatoverschrijdende organisaties te maken kunnen hebben met verschillende nationale privacywetten. De oplossing daarvoor

[204] Zie Prins 2003, p. 69-73.
[205] Hustinx 2004, p. 270-272.
[206] De Hert & Gutwirth 2004, p. 587-631.
[207] Dit kwam naar voren in de bijeenkomst met domeindeskundigen.

zou kunnen zijn een country-of-origin regel, op basis waarvan slechts een privacywet, namelijk die van het land van de hoofdvestiging, van toepassing zou zijn op de verwerkingen.

Ook blijkt uit het Implementatierapport dat er kritiek is op de werkbaarheid en onduidelijkheid van het criterium betreffende het gebruik van al dan niet geautomatiseerde middelen die zich bevinden op het grondgebied van een lidstaat. De Commissie sluit in dat verband niet uit dat er moet worden gezocht naar een ander criterium:

> 'As regards the "use of equipment" the Commission is aware that this criterion may not be easy to operate in practice and that it needs further clarification. Should such clarification not be sufficient to ensure its practical application, it might in due course be necessary to propose an amendment creating a different connection factor in order to determine the applicable law'.[208]

In de literatuur over de Wbp wordt enige aandacht besteed aan een en ander. Terstegge[209] geeft aan dat er, ondanks de door de richtlijn beoogde harmonisering, nog sprake is van verschillen in de wet- en regelgeving, die nog eens worden uitvergroot door verschillende opvattingen van toezichthouders en nationale rechters – dit wordt bevestigd door Cuijpers[210] en de Artikel 29 Werkgroep.[211] Als gevolg daarvan is het voor verantwoordelijken die in meer dan een lidstaat activiteiten ontplooien volgens Terstegge problematisch om de wetgeving na te leven. En dit betekent volgens hem dat:

> 'instead of lifting barriers for the free flow of personal data within the European Union, the current European systeem of data protector tends to create barriers by impossing different obligatiefonds and procedures on data controllers which operate in more than one member state'.[212]

Het probleem of knelpunt dat Terstegge schetst betreft in algemene zin alle verantwoordelijken met vestigingen in meerdere lidstaten en meer in het bijzonder multinationals. Als oplossing doet Terstegge voorstellen voor een 'home country control-system'. In dit systeem, dat overeenkomt met het in het Implementatierapport als 'country of origin' aangeduide systeem, hoeven de verwerkingen, behoudens enkele uitzonderingen, alleen te voldoen aan de wetgeving van het land waar de (Europese) hoofdvestiging zich bevindt. Het probleem dat daarmee wordt opgelost betreft enerzijds de gehoudenheid voor verantwoordelijken om bij verschillende privacytoezichthouders langs te gaan en anderzijds het risico dat een lidstaat barrières opwerpt voor de doorgifte van persoonsgegevens naar derde landen:

> 'This would eliminate the *Tour d'Europe* as well as a possible veto of a single member state in relations to international data transfers'.[213]

Dit probleem en de voorgestelde oplossing wordt in ook een enkele andere publicatie, zoals die van Cuijpers,[214] Kroes[215] en Van der Putt[216] in een boekje over de werking van de Wbp in concern-verband, aangestipt en kort besproken. Daarbij wijst de eerste van deze auteurs erop dat het 'home country control' systeem niet nieuw is, want het betreft een van de uitgangspunten van de richtlijn elektronische handel.[217] Uit

---

[208] Implementatierapport, p. 17.
[209] Terstegge 2002, p. 257-259.
[210] Cuijpers 2003, p. 114.
[211] Art. 29 Werkgroep 2002.
[212] Terstegge 2002, p. 257.
[213] Terstegge 2002, p. 259.
[214] Cuijpers 2003, p. 121-122.
[215] Kroes 2003, p. 29.
[216] Van der Putt 2003, p. 31-34.
[217] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van diensten van de informatiemaatschappij met name elektronische handel in de interne markt, *PbEG* 2000, L178/1.

deze en andere literatuur, zoals een uiteenzetting van problemen bij zgn. clinical trials door Van Quathem,[218] blijkt dat dit vooral als knelpunt wordt ervaren waar het gaat om internationale concernverhoudingen en andere internationale constructies. Meer daarover in hoofdstuk 5 over de private sector.

Een andere, verdergaande oplossing van dit knelpunt wordt gesuggereerd door Thijssen.[219] Zij stelt voor om artikel 4, eerste lid, Wbp zodanig aan te passen dat de wet alleen de gegevens beschermt die in een vestiging van de verantwoordelijke in Nederland worden verwerkt. En dus niet meer de gegevens die in een of ander buitenland worden verwerkt in het kader van activiteiten van een vestiging van de verantwoordelijke in Nederland.

Schreuders en Blok[220] bespreken hetzelfde knelpunt, maar in een andere context. Zij stellen vast dat de Wbp van toepassing kan zijn op veel partijen die betrokken zijn bij communicatie via internet. De auteurs laten in het midden of dat op zichzelf als knelpunt moet worden gezien – hoewel zij wel spreken van ongerijmdheden. Zij wijzen op knelpunten die het gevolg zijn van de toepassing van de wet op zoveel verschillende partijen, zijnde knelpunten met betrekking tot de doorgifte van persoonsgegevens naar derde landen. Ook Berkvens[221] laat zich in die zin uit. Over de indertijd nog niet besliste Lindqvist-zaak merkt hij op dat de partijen die betrokken zijn betrokken bij het elektronisch berichtenverkeer met een 'flinke rechtsonzekerheid' blijven zitten.

Schreuders en Blok wijzen er ook op dat transporteurs die in Nederland zijn gevestigd anders worden behandeld dan transporteurs van buiten de EU. Als het gaat om alleen de doorvoer van gegevens vallen de in Nederland gevestigde transporteurs wel onder de wet, terwijl de transporteurs van buiten de EU daar geen last van hebben. Ook dit wordt door deze auteurs aangeduid als een ongerijmdheid. Het is niet ondenkbaar dat daardoor bijvoorbeeld de concurrentie wordt verstoord tussen enerzijds in Nederland of elders in de EU gevestigde telecommunicatiedienstenaanbieders en anderzijds Amerikaanse telecommunicatiedienstenaanbieders. In de literatuur blijken dergelijke specifieke knelpunten echter niet.

Blok[222] wijst er verder op dat de richtlijn en dus ook de wet als gevolg van deze toepassingsregels een erg ruime werkingssfeer heeft. Een gevolg daarvan is dat de wet van toepassing kan zijn op verwerkingen die nauwelijks een band hebben met de EU. Als voorbeeld noemt hij de verwerking van gegevens over Amerikaanse betrokkenen ten behoeve van een Amerikaanse overheidsinstelling, waarbij gebruik wordt gemaakt van middelen die zich bevinden in de EU. Verder wijst deze auteur erop dat dezelfde toepassingsregels ertoe kunnen leiden dat een website in het Nederlands en gericht op Nederlanders daarmee nog niet onder de Wbp hoeft te vallen.

De Vries[223] noemt hetzelfde probleem en geeft als voorbeelden de situatie van het callcenter in Nederland dat als bewerker in opdracht van verschillende verantwoordelijken in andere lidstaten telefoongesprekken met klanten opneemt. Deze bewerker zal telkens te maken krijgen met een andere nationale privacywet, al naar gelang de eindbestemming van het binnenkomende telefoongesprek. En dat betekent dat deze bewerker de ene keer toestemming moet vragen en de andere keer kan volstaan met het geven van relevante informatie. Ook het 'gebruik-van-middelen criterium' van artikel 4, tweede lid, Wbp ziet zij als een probleem: het schiet tekort of is niet goed handhaafbaar.

---

[218] Van Quathem 2005, p. 155-161.
[219] Thijssen 2005, p. 110-113.
[220] Schreuders & Blok 2002, p. 455-457.
[221] Zie Prins 2003, p. 59-62.
[222] Blok 2005a, p. 297-304.
[223] De Vries 2006, p. 265-267.

Winkelhorst denkt daar anders over.[224] Hij stelt dat de zoekmachine Google op grond van het dit criterium zich in de EU aan de richtlijn en in Nederland dus aan de Wbp moet houden. Hij kan zich daarin, vanuit het perspectief van de bescherming van de betrokkene, wel vinden omdat daarmee:

> 'de burger mogelijk niet zo vogelvrij [is] als tot nu toe werd aangenomen'.

In een brief aan de Minister doet het Cbp[225] ten slotte een voorstel voor de oplossing van een deel van dit probleem, namelijk waar het toepassing van de meldplicht betreft op verantwoordelijken die in verschillende lidstaten zijn gevestigd. Het Cbp stelt voor dat er een standaard meldformulier wordt ontwikkeld waarmee de verwerkingen in de verschillende lidstaten eenmalig kan melden.

Een knelpunt voor verantwoordelijken met vestigingen in meerdere lidstaten is dat verschillende nationale privacywetten van toepassing zijn op de verwerkingen van deze vestigingen. Verder kunnen als knelpunten worden genoemd de omstandigheid dat de Wbp enerzijds van toepassing kan zijn op verwerkingen die weinig verband houden met Nederland, terwijl anderzijds de wet niet van toepassing kan zijn op verwerkingen die wel specifiek verband houden met Nederland. Een enkele auteur ziet de territoriale toepassing van de wet niet als probleem maar als een voordeel. Het Cbp staat een standaard meldformulier voor waarmee verwerkingen in verschillende lidstaten kunnen worden gemeld.

Journalistieke, artistieke en literaire doeleinden

Voorafgaand aan de inwerkingtreding van de Wbp heeft Kabel[226] enige kritische opmerkingen gemaakt over de wijze waarop de nationale wetgever invulling heeft gegeven aan de ruimte die de richtlijn laat met betrekking tot de toepassing van de wet op verwerkingen met journalistieke, artistieke of literaire doeleinden. Zijn kritiek is vooral gericht tegen de keuze van de nationale wetgever om de op de verantwoordelijke rustende meld- en informatieplichten (art. 27 en 33-34) niet van toepassing te doen zijn op verwerkingen ten behoeve van deze journalistieke, artistieke of literaire doeleinden. Hij wijst erop dat de niet-toepasselijkheid het toezicht op de naleving van de wel geldende bepalingen onzeker maakt. Dit omdat:

> '[h]et immers slechts van toevalligheden [zal] kunnen afhangen of betrokkene op de hoogte kan zijn van (niet-openbare) verwerking van zijn persoonsgegevens door pers en omroep. [...] Zonder die [transparantie]plichten, zijn de rechten van betrokkene betrekkelijk waardeloos en daarmee ook de mogelijkheid tot individuele handhaving voor de burgerlijke rechter van de specifieke kwaliteitsplichten en toelaatbaarheidsvereisten.

Verder wijst Kabel erop dat de Wbp de verwerking van bijzondere of gevoelige gegevens voor journalistieke, artistieke of literaire doeleinden toestaat omdat het dan volgens de MvT[227] gaat om een zwaarwegend algemeen belang in de zin van artikel 8, vierde lid, van de richtlijn en artikel 23, onder e, Wbp. De vraag is dan of alle journalistiek, inclusief de wat 'lichtere' roddelbladen, onder deze uitzondering vallen. Verder vraagt Kabel zich af of het terecht is dat de doorgiftebepalingen niet van toepassing zijn. De conclusie van zijn beschouwing is evenwel dat er weinig echte conflicten hierover zijn en dat er dus geen sprake lijkt te zijn van een groot probleem. Alleen waar het gaat om publicatie van namen van daders en slachtoffers van misdrijven zou er een knelpunt kunnen zijn.

Winkelhorst & Ter Linden-Smit[228] stellen vast dat de regels met betrekking tot verwerkingen voor voornoemde journalistieke, artistieke en literaire doeleinden onvoldoende duidelijk zijn als het gaat om publica-

[224] Winkelhorst 2005, p. 146-154.
[225] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[226] Kabel 1997, p. 76-80.
[227] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 74.
[228] Winkelhorst & Van der Linden-Smith 2004, p. 627-631.

ties op internet. In zijn annotatie bij het Lindqvist-arrest van het Europees Hof van Justitie[229] suggereert Zwenne[230] dat de uitzondering voor verwerkingen met journalistieke, artistieke en literaire doeleinden ruimer worden geïnterpreteerd, zodat ook websites daaronder vallen. Volgens deze auteur is dit wenselijk omdat het Hof in zijn arrest weliswaar heeft aangegeven dat de doorgifteregels in het geval van de desbetreffende website niet van toepassing waren. Maar nog los van de vraag hoe dit in andere gevallen zal uitpakken vindt deze auteur dat daarmee nog niet het probleem is opgelost dat op veel, in termen van privacy risicoloze, websites wel onnodige en veelal niet te handhaven verplichtingen rusten, zoals met name de meldplicht.

Ook het Cbp bespreekt in een verkennende studie[231] uitgebreid in hoeverre publicaties op internet vallen onder de uitzondering voor verwerkingen met journalistieke, artistieke of literaire doeleinden. Een eenduidige conclusie levert deze studie niet op: of een internetpublicatie onder deze uitzondering valt hangt af van de mate waarin kan worden gezegd dat er een algemeen maatschappelijk belang wordt gediend met de desbetreffende publicatie. In de verkenning worden enkele criteria geformuleerd aan de hand waarvan de toezichthouder kan bepalen of hij zich bezig zal gaan houden met publicaties op het internet.

De gedeeltelijke niet-toepassing van de wet op verwerkingen met journalistieke, artistieke en literaire doeleinden leidt tot vragen over de rechtsbescherming en handhaving van de bepalingen die wel van toepassing zijn, maar lijkt geen aanleiding te geven tot knelpunten. De reikwijdte van de uitzondering voor verwerkingen met journalistieke, artistieke en litereaire doeleinden is onduidelijk en kan worden gezien als knelpunt. Een ruimere interpretatie van deze journalistieke, artistieke en literaire doeleinden wordt gesuggereerd om websites meer buiten de werking van de wet te brengen, zodat deze geen onderwerp zijn van onnodige en niet te handhaven verplichtingen. In dit verband heeft het Cbp enkele criteria geformuleerd.

4.3 Normatieve kaders

4.3.1 Wijze van normering

Verantwoordelijke en verantwoordelijkheid

Er zijn, blijkt uit de literatuur, in de praktijk vragen over wie er zich moet houden aan de materiële normen van de wet, ofwel vragen over wie heeft te gelden als ‘ de verantwoordelijke’ in de zin van de wet. Schreuders en Gardeniers[232] menen dat het in de meeste gevallen wel duidelijk is wie de verantwoordelijke in de zin van de wet is. Maar er zijn toch ook situaties waarin volgens hen lastig is te bepalen wie in de praktijk feitelijk zorg draagt voor naleving van de wet. Zij noemen drie situaties waarin daarvan sprake kan zijn: (1) situaties die zich vooral in de grotere organisaties voordoen en waarin het feitelijk beheer van en verantwoordelijkheid over informatiesystemen en gegevensverwerkingen niet altijd duidelijk is; (2) situaties waarin verschillende partijen met elkaar samenwerken en waarin het niet meer goed duidelijk is wie voor welke verwerking verantwoordelijk is; [233] en (3) situaties waarin via internet verwerkingen worden gedaan door, zoals bij peer-to-peer programma’s of aanbieders die faciliteiten beschikbaarstelling waarop gebruikers zelf gegevens kunnen invullen (bijv. sollicitatiesites).

---

[229] EHvJ 6 november 2003, (Bodil Lindqvist) C101/01).
[230] Zwenne 2004, p. 66-69.
[231] Versmissen, Schinkel & Kraaij 2006
[232] Schreuders & Gardeniers 2005, p. 260-262.
[233] In België biedt de zg. SWIFT-casus een interessant voorbeeld van een geval waarin er vragen waren over wie had te gelden als verantwoordelijke en wie als bewerker; zie de Commissie voor bescherming van de persoonlijke levenssfeer, Advies Nr. 37/2006 van 27 september 2006 www.privacycommission.be.

Van der Putt[234] bespreekt soortgelijke situaties, waarbij in concern- of joint venture-constructies moeilijk blijkt te kunnen worden vastgesteld wie waarvoor verantwoordelijk is. Ook Thijssen[235] gaat in op deze specifieke problemen. In de verkenning van het Cbp[236] over internetpublicaties wordt verder gewezen op problemen met het identificeren van wie heeft te gelden als de verantwoordelijke voor verwerkingen op het internet. Meer daarover in hoofdstuk 5 over de private sector.

Er worden knelpunten gesignaleerd waar het gaat om het vaststellen van wie hebben te gelden als verantwoordelijken en op wie de materiële normen van de wet dus primair van toepassing zijn. Deze doen zich met name voor waar het gaat joint venture-constructies of in de context van internet.

Geen kristallisatiepunt voor de rechtspraktijk

Over de normatieve kaders van de Wbp maken De Hert & Gutwirth[237] een aantal opmerkingen die erop duiden dat de wet volgens hen in elk geval niet het kristallisatiepunt biedt dat de wetgever voor ogen had.[238] Zij stellen dat de Wbp geen wet is van gebieden en verbieden, en dat de kracht ervan niet ligt in het bewerkstelligen van materiële rechtvaardigheid. Volgens hen ademt de wet de boodschap uit dat gegevensverwerkingen zijn toegestaan als maar aan een aantal procedurele spelregels is voldaan. De wet ziet vooral op procedurele rechtvaardigheid, en dit verklaart volgens de auteurs waarom in de Wbp maar weinig duidelijke zwart-wit bepalingen staan of verbodsbepalingen. Op dit punt is de wet daardoor niet zo sterk:

> 'Duidelijke antwoorden geven is niet de sterkste kant van de Wbp. Dat moet de verantwoordelijke zelf maar uitmaken, eventueel gecontroleerd door de geregistreerde die het Cbp of de rechter kan inschakelen.'

De auteurs duiden de wet aan als 'een erg bedrijfs- en overheidsvriendelijke kopie van de Europese richtlijn', die in vergelijking met de wetgeving in andere lidstaten 'in dit bedje ziek' is. Waar het gaat om de criteria aan de hand waarvan wordt bepaald of een gegevensverwerking rechtmatig is of niet, spreken deze auteurs over 'soepele criteria'. Veel verwerkingen worden volgens hen gebaseerd op de belangenafweging van artikel 8, onder f, van de wet, welke bepaling zij karakteriseren als 'weinigzeggend' en waarover zij verder opmerken, dat:

> '[d]eze bepaling [..] de in de sfeer van de grondrechten onwenselijke gedachte uit [ademt] dat alles een kwestie is van afweging van gelijke belangen'

Onwenselijk vinden de auteurs deze gedachte, zo blijkt uit een voetnoot, omdat juist grondrechten aangeven dat in sommige gevallen aan bepaalde belangen meer gewicht toekomt dan aan andere belangen. Daarbij tekenen zij aan dat niet elke rechtmatige of onrechtmatige verwerking van persoonsgegevens een inbreuk vormt op grondrechten. Hoewel de beide auteurs op zichzelf niet tegen een dergelijke oriëntatie op procedure zijn, menen zij dat zonder hardere, materiële normen of grenzen er een element ontbreekt.

Schreuders en Gardeniers[239] wijzen op meer praktische knelpunten. Hoewel volgens deze auteurs het publiekrechtelijk georiënteerde stramien van de materiële normen van de artikelen 6 t/m 9 en 11 Wbp op zich vrij helder is, blijkt het in de praktijk bepaald niet eenvoudig om ermee te werken. Volgens hen wordt dit verklaard doordat de wet ervan uitgaat dat bij iedere afzonderlijke verwerking wordt nagegaan of deze in overeenstemming is met de wet. En daarbij komt dat de toe te passen normen een erg open karakter hebben, reden waarom:

---

[234] Van der Putt 2003, p. 31-34; zie ook in hetzelfde boekje de casusbesprekingen op p. 123-151.
[235] Thijssen 2002, p. 84-88.
[236] Cbp, Publicatie van persoonsgegevens op internet. Een verkenning, 17 mei 2006, p. 30-33.
[237] De Hert & Gutwirth 2004, p. 587-631.
[238] Vgl. par. 3.3.2 van dit rapport.
[239] Schreuders & Gardeniers 2005, p. 260-262.

> 'het in de praktijk van alle dag nagenoeg ondoenlijk is om volledig uitvoering te geven aan de materiële normen. De blijkbaar in de Wbp opgesloten verwachting dat personen en organisaties bij elke afzonderlijke verwerking het stramien van de Wbp zullen doorlopen en dat het voor iedereen die met persoonsgegevens werkt mogelijk is om handen en voeten te geven aan de vele open normen is, in strikte zin, eenvoudig weg niet realistisch. In die zin vergt de Wbp meer van mensen dan menselijk haalbaar is. En in die zin is de Wbp, evenals de WPR, een onderwerp voor specialisten'.

In de praktijk leidt dit tot een aantal, niet altijd weloverwogen strategieën en handelswijzen met betrekking tot de verwerking van persoonsgegevens. De auteurs merken op dat deze tot gevolg hebben dat er strengere normen worden gehanteerd dan de Wbp verlangt. Een voorbeeld daarvan is het gebruik dat wordt gemaakt van de vrijstellingen op de meldplicht. Wanneer van deze vrijstellingen gebruik wordt gemaakt hoeft het stramien van de materiële normen van de Wbp niet te worden doorlopen, omdat de concrete regels al uit het Vrijstellingsbesluit voortvloeien. Het resultaat is dat de verantwoordelijke kiest voor een strenger regime met beperkingen, namelijk het regime dat voortvloeit uit het Vrijstellingsbesluit. Daarnaast wijzen deze auteurs erop dat in veel gevallen niet wordt gedifferentieerd ten aanzien van de mogelijke verwerkingsgronden (zoals toestemming, uitvoering overeenkomst of gerechtvaardigd belang[240]), waardoor ook de mogelijkheden om te verwerken worden beperkt. Ten slotte wijzen de auteurs erop dat de Wbp ook als 'privacyexcuus' wordt gebruikt: om lastige afwegingen uit de weg te gaan verschuilen verantwoordelijken zich achter het argument dat het 'van de privacywet niet mag'. De beide auteurs komen dan ook tot de conclusie dat::

> '[e]en rechttoe rechtaan toepassing van het publiekrechtelijk stramien van de Wbp [...] voor de praktijk te hoog gegrepen [lijkt]'.

Ook waar de rechtspraak en de besluiten van het Cbp aanknopingspunten bieden voor de toepassing van de materiële normen, kan de praktijk daar volgens hen maar slecht mee uit de voeten. En hoewel het volgens hen niet zo is dat er in die praktijk onzorgvuldig wordt omgegaan met persoonsgegevens, menen zij dat het te complexe normatieve en niet effectief werkende kader zijn doel voorbij schiet. Zij vinden dan ook dat er binnen de bandbreedte van de richtlijn moet worden gezocht naar 'een meer praktische benadering, mogelijk met concrete uitwerkingen'. Ofwel 'van wetenschap voor specialisten naar praktische randvoorwaarden voor gegevensbescherming in de praktijk'.

Het door Schreuders en Gardeniers geschetste beeld van de Wbp wordt bevestigd in verschillende publicaties. In een (afstudeer)onderzoek naar de naleving van de Wbp in zorginstellingen komt Van der Pol[241] tot de conclusie dat de wet zonder specialistische hulp voor een gemiddelde organisatie 'gewoonweg onmogelijk' is te gebruiken als ijkpunt voor privacybescherming. Door de open normen kunnen organisaties volgens deze auteur niet zelf vaststellen of zij aan de wet voldoen. Merkus[242] geeft aan dat verwerkingen van bijvoorbeeld werknemergegevens in het kader van een due diligence onderzoek – een onderzoek van een onderneming dat wordt gedaan in het kader van een overname – door de toezichthouder maar in zeer beperkte mate geoorloofd worden geacht en daarmee beperkend werkt bij een overname.

Een van de in de wet vastgelegde materiële normen, te weten het doelbindingsbeginsel van artikel 9 jo. 7 Wbp, is onderwerp van een korte beschouwing van Blok.[243] Hij stelt dat dit beginsel het de belangrijkste materiële norm is op het gebied van de verwerking van persoonsgegevens en dat het dan ook een cruciale rol speelt bij de beoordeling van de rechtmatigheid daarvan. Toch is dit beginsel, zoals ook al bleek in het WPR evaluatieonderzoek van Overkleeft-Verburg,[244] onderbelicht in de toetsingspraktijk van rechters en

---

[240] Resp. art. 8, onder a, b of f, Wbp.
[241] Van der Pol 2006, p. 110-114.
[242] Merkus 2002, p. 14-18.
[243] Blok 2003b, p. 45-59.
[244] Overkleeft-Verburg 1995.

toezichthouder. Er wordt, stelt Blok vast, niet of nauwelijks gekeken naar de doeleinden die een gegevensverwerker oorspronkelijk op het oog had. Als wordt getoetst of is voldaan aan het doelbindingsbeginsel wordt gekeken naar de rechtmatigheid van de verwerking: als deze rechtmatig wordt geoordeeld wordt vervolgens aangenomen dat de verwerking in overeenstemming is met het doelbindingsbeginsel. En dat is de omgekeerde volgorde. Als voorbeeld noemt deze auteur een al wat oudere uitspraak van de rechtbank Leeuwarden, [245] waarin nog onder de WPR werd geoordeeld dat een goede uitvoering van de taak van een curator een maatschappelijk belang betreft dat de gevraagde gegevensverstrekking rechtvaardigde:

> 'Dit maatschappelijk belang rechtvaardigt de gevraagde verstrekkingen. Deze gegevensversterkking moet dan ook worden geacht voort te vloeien uit het doel van de registratie.'

Blok komt tot de conclusie dat de verantwoordelijke in de praktijk slecht in beperkte mate is gebonden aan de door hem gespecificeerde doeleinden omdat het niet-onverenigbaarheidscriterium een tamelijk ruim begrip is. Ook stelt hij vast dat de door de verantwoordelijke gespecificeerde doeleinden maar een beperkte relevantie hebben bij de beoordeling van de rechtmatigheid van de verwerkingen. Ten slotte meent hij dat in het tweede lid van artikel 9 Wbp ten onrechte de mate van verwantschap van de verantwoordelijke met degene die de gegevens na verstrekking verder zal verwerken, niet ook als criterium is opgenomen.

De wet heeft volgens sommige auteurs een te eenzijdig procedureel karakter en biedt te weinig harde materiële normen. Volgens andere auteurs is de wet te onpraktisch omdat deze ervan uit gaat dat bij elke verwerking aan de normen van de Wbp wordt getoetst, en omdat de normen te vaag zijn. Als gevolg daarvan wordt vaak gekozen voor strengere voorwaarden dan nodig. Een auteur meent dat het doelbindingsbeginsel maar beperkte betekenis heeft. De wet wordt gezien als een wet voor specialisten.

Aansluiting met andere wetgeving

Er is voorafgaand aan de inwerkingtreding van de Wbp al uitvoerig gediscussieerd over de gebrekkige inbedding van de wet in het rechtsstelsel of de aansluiting bij het overige recht.[246] De implementatie van de richtlijn werd aangemerkt als goed moment om een betere aansluiting op de andere delen van het recht te realiseren.[247] Hoewel de wetgever daar uitvoerig bij heeft stilgestaan[248] komt uit de literatuur over de wet naar voren dat deze inbedding of aansluiting op enkele onderdelen toch nog niet optimaal is. Dit wordt deels verklaard door het te algemene karakter van de wet, dat het gevolg is van de in de het voorgaande[249] besproken omnibusbenadering. Als gevolg daarvan blijkt het lastig te zijn om de open normen van de wet consistent in te vullen en ook wel om te bepalen op wie deze normen van toepassing zijn.

De Koning en De Vries[250] gaan in op de verhouding tussen de Wbp en de Databankenwet – de wet waarin een een *sui generis* recht van intellectuele eigendom wordt gecreëerd voor databanken.[251] Zij stellen vast dat er niet of nauwelijks geschillen aan de rechter worden voorgelegd die betrekking hebben op het spanningsveld tussen enerzijds databankrechten en anderzijds privacyrechten. Maar daaruit mag volgens deze auteurs niet worden geconcludeerd dat de gelijktijdige toepassing van de Databankenwet en de Wbp vlekkeloos verloopt. Van knelpunten zou volgens de beide auteurs sprake kunnen zijn waar de rechthebbende

---

[245] Rechtbank Leeuwarden 3 mei 1993, *NJ* 1994.
[246] Vgl. Overkleeft-Verburg 1995.
[247] Verhey 1997, p. 254.
[248] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 37-9; *Kamerstukken II* 1998-1999, 25 892, nr. 6, 15; *Handelingen II* 28 november 2000, p. 24-1793; *Handelingen I* 3 juli 2000, p. 34-1599.
[249] Zie par. 4.2.2 van dit rapport.
[250] Koning en de Vries 2003, p. 52-58.
[251] Wet van 8 juli 1999, houdende aanpassing van de Nederlandse wetgeving aan richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken, *Stb.* 1999, 303.

van de databank met persoonsgegevens niet dezelfde persoon is als de verantwoordelijke. Verder wijzen de auteurs erop dat rechthebbenden zich niet altijd er van bewust zijn dat zij ook verantwoordelijke kunnen zijn, en omgekeerd, waardoor de naleving van de beide wetten wordt bemoeilijkt.

Ook Prins[252] gaat in op de verhouding tussen databankenrecht en persoonsgegevens. In een beschouwing waarin concepten van eigendom en privacy worden geanalyseerd wijst zij op de soms tegengestelde verwachtingen en aanspraken die aan de databankenrichtlijn (96/9/EG)[253] en de privacy-richtlijn worden ontleend. Maar zij presenteert dit niet zozeer als knelpunt van de wet of de richtlijn, maar veeleer als een illustratie van de verschillende uitgangspunten en implicaties van de beide richtlijnen.

Van der Zijde[254] bespreekt de verhouding tussen de Wbp en de Telecommunicatiewet, en de wetgeving betreffende verkoop op afstand en elektronische handel. Zij stelt vast dat er, met name waar het gaat om de in de verschillende wetten gebruikte toestemmingsbegrippen, sprake is van een gebrekkige aansluiting. Verder wijst zij op enige lacunes in de wetgeving, zoals in de verhouding tussen het doelbindingsvereiste van artikel 9 Wbp in relatie met de regeling betreffende het gebruik van elektronische contactgegevens van artikel 11.7, tweede lid, Wbp. Over dezelfde wetgeving merkt het Cbp[255] op dat de begrippen uit de Wbp niet overeenkomen met die van de Aanpassingswet inzake richtlijn elektronische handel,[256] bijvoorbeeld waar het gaat om de geadresseerde van de beide wetten. Deze problemen doen zich vooral voor als het gaat om direct marketing in de private sector. Daarom meer hierover in hoofdstuk 5.

Over de aansluiting met andere, reeds in het kader van de evaluatie van de WPR besproken wetten, zoals de Wob, de Archiefwet en sectorale wetten is verder weinig literatuur te vinden. Wel bleek uit de bijeenkomst met domeindeskundigen dat de Wbp volgens velen in elk geval niet beter aansluit bij de overige wetgeving dan de WPR. Dit lijkt evenwel vooral te maken te hebben met het algemene karakter van de wet en de daarin gehanteerde open normen, en niet zozeer met uiteenlopende begrippenapparaten of het ontbreken van verwijs- en schakelbepalingen.

4.3.3 Bijzondere gegevens

Definiëring en afbakening bijzondere of gevoelige gegevens

Holvast en Rodrigues[257] bespreken de strengere regels die gelden voor bijzondere of gevoelige gegevens. Een eerste, meer principieel knelpunt dat zij noemen betreft de omstandigheid dat de gevoeligheid van gegevens afhankelijk is van de context waarin de gegevens worden gebruikt. De aantekening van een docent dat een leerling verzuimt in verband met een verkoudheid wordt nauwelijks als gevoelig gezien, maar is dat wel voor de wet. Hetzelfde geldt voor de foto's in het smoelenboek op het intranet van een bedrijf of instelling. Ook deze gegevens zullen niet als gevoelig worden gezien maar zijn dat voor de wet wel omdat het ras daaruit blijkt. De auteurs wijzen er verder op dat ook het Cbp in een brief aan de Minister van Justitie heeft aangegeven dat het regime met betrekking tot sommige bijzondere gegevens als te knellend wordt ervaren.[258] Om deze redenen menen deze auteurs dat:

> 'het gebruik van een categorie van bijzondere gegevens [..] zowel generiek als specifiek een minder geslaagd onderdeel van de wet is.

---

[252] Prins 2006, p. 229-230.
[253] Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken, *PbEG* 1996 L 077/20.
[254] Van der Zijde 2006, p. 121 e.v.
[255] Cbp, Publicatie van persoonsgegevens op internet. Een verkenning, 17 mei 2006, p. 20.
[256] *Stb.* 2004, 2002.
[257] J. Holvast & P.R. Rodrigues 2005, p. 263-267.
[258] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.

Zij pleiten ervoor dat daar in de evaluatie van de wet en de richtlijn aandacht wordt gegeven. In voornoemde brief wijst het Cbp op de knelpunten met betrekking tot de verwerking van de bijzondere gegevens als accountants en auditors een verificatie- of nalevingsonderzoek doen in de zorg. Ook geeft de toezichthouder aan dat de Nationale ombudsman soortgelijke problemen heeft als er bijzondere gegevens in zin onderzoeken beschikbaar komen. Het Cbp doet de Minister van Justitie het verzoek te bezien of, deze knelpunten kunnen worden verholpen door daarvoor een ontheffingsgrond in de Wbp op tenemen, danwel een regeling in de Awb en/of aanpassing van bijzondere wetten. Een soortgelijke oplossing wordt door Smits[259] voorgesteld waar het gaat om de als knelpunten ervaren beperkingen die gelden met betrekking tot de verwerking van gevoelige gegevens in het kader van drugs- en alcohol-testen. Deze auteur meent dat gebruik zou moeten worden gemaakt van de ontheffingsmogelijkheid van artikel 23, eerste lid, onder e, Wbp.

Voor andere verwerkingen van bijzonder gegevens, met name strafrechtelijke gegevens, signaleert het Cbp eveneens knelpunten die door de wetgever zouden kunnen worden opgelost. In enkele brieven[260] verzoekt het de minister om de uitzonderingen op het verbod van de verwerking van strafrechtelijke gegevens fijnmaziger in te vullen, teneinde zo een aantal veel voorkomende en maatschappelijk geaccepteerde gegevensverwerkingen van deze gegevens niet meer te onderwerpen aan een zgn. voorafgaand onderzoek door het Cbp.[261] Als voorbeelden van verwerkingen die niet meer aan zo een onderzoek zouden moeten worden onderworpen noemt het Cbp de verwerkingen van strafrechtelijke gegevens ten behoeve van derden, zoals het verstrekken van strafrechtelijke gegevens aan de politie ten behoeve van de aangifte van een strafbaar feit, het verstrekken van strafrechtelijke gegevens aan inspecties en toezichthouders voor zover dit nodig is voor de uitoefening van hun taak en het uitwisselen van strafrechtelijke gegevens tussen partijen in samenwerkingsverbanden voor zover betrokken partijen allen op grond van hun eigen taken en bevoegdheden over deze gegevens mogen beschikken.

In het Implementatierapport zet de Commissie[262] uiteen dat er met betrekking tot gevoelige gegevens implementatieverschillen zijn waar het gaat om arbeidsrelaties, alsmede dat sommige lidstaten de desbetreffende bepaling uit de richtlijn niet (helemaal) goed hebben geïmplementeerd. Nederland valt daar echter niet onder:

> 'This provision allows Member States to make exceptions from the general rule that sensitive data should not be processed, where such processing is necessary to carry out the obligations and specific rights of the controller in the field of employment law, but only subject to adequate safeguards being put in place. In some Member States, these requirements are met through specific data protection legislation in the employment context, which is either quite comprehensive (eg. Finland) or regulates particular issues (eg. health legislation in Denmark and the Netherlands). In other Member States, the situation is less clear.'

Over de perceptie van wat als gevoelig wordt gezien wordt maakt Nagel[263] enkele opmerkingen Hij wijst erop dat uit verschillende onderzoeken van de Consumentenbond blijkt dat onder andere gegevens over financieel vermogen, inkomen, schulden door betrokkenen als privacygevoelig worden aangemerkt, terwijl dat voor gegevens over ras veel minder geldt. Er is dus kennelijk een zekere discrepantie tussen wat de wet als extra beschermenswaardig ziet en wat de betrokkenen als bijzonder privacygevoelig beschouwen. Meer over de problematiek met betrekking tot gevoelige gegevens in hoofdstuk 7 over de semi-publieke sector.

---

[259] Smits 2006, p. 115-120.
[260] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086 en Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
[261] Art. 22, vierde lid, onder c, Wbp.
[262] Implementatierapport, p. 14.
[263] Nagel 2006, p. 268-270.

Het aanduiden van een hele categorie van gegevens als bijzondere gegevens leidt in de praktijk tot knelpunten omdat de gevoeligheid van bijzondere gegevens contextafhankelijk is. Het Cbp acht het regime van bijzondere gegevens op onderdelen te knellend en stelt voor dit te verhelpen door voor bepaalde gegevensverwerkingen een ontheffingsgrond op te nemen in de Wbp, of door aanpassing van de Awb of bijzondere wetten. Voor een aantal specifeike verwerkingen doet de toezichthouder de suggestie voor een fijnmaziger invulling van uitzonderingen op het verwerkingsverbod van deze gegevens. Uit onderzoek van de Consumentenbond blijkt discrepantie tussen wat de wet als extra beschermenswaardig ziet en wat betrokkenen als bijzonder privacygevoelig beschouwen.

Uitdrukkelijke en ondubbelzinnige toestemming

Waar het gaat over de normatieve kaders wordt in het Implementatierapport, behalve op het probleem dat een aantal lidstaten de richtlijn niet juist heeft geïmplementeerd, alleen gewezen op de onduidelijkheden die er bestaan met betrekking tot uitleg en invulling van enerzijds 'ondubbelzinnige' en anderzijds 'uitdrukkelijke' toestemming van respectievelijk artikel 7, onder a, en artikel 8 , tweede lid, onder a, van de richtlijn, ofwel de artikelen 8, onder a, en 23, eerste lid, onder a, Wbp. In het rapport merkt de Commissie op dat de beide begrippen, met name in on line-omgevingen, moeten worden opgehelderd:

> 'The notion of "unambiguous consent" (Article 7 (a)) in particular, as compared with the notion of "explicit consent" in Article 8, needs further clarification and more uniform interpretation. It is necessary that operators know what constitutes valid consent, in particular in on-line scenarios.

De Artikel 29 Werkgroep[264] heeft, mede in antwoord op het Implementatierapport, aangegeven deze en andere begrippen te willen verduidelijken.

De interpretatie van de verschillende toestemmingsvarianten in de richtlijn en de wet kan tot knelpunten aanleiding geven, met name in een online-omgeving.

Vitaal belang

In zijn brief met voorstellen voor wijziging van de Wbp wijst het Cbp[265] op nog een ander knelpunt, namelijk dat de vrijwaring van een vitaal belang van de betrokkene wel een grondslag voor de verwerking van persoonsgegevens is, maar het doorbreekt niet het verbod op het verwerken van bijzondere persoonsgegevens.[266] En hoewel het Cbp het onwaarschijnlijk vindt dat dit iemand ervan zal weerhouden gegevens te verstrekken in gevallen waarin acuut gevaar voor iemands leven of gezondheid dreigt, acht de toezichthouder het niettemin wenselijk om deze uitzondering expliciet in de Wbp te regelen.

Het ontbreken van een regeling op grond waarvan bijzondere gegevens kunnen worden verwerkt als dat nodig is ter vrijwaring van een vitaal belang van de betrokkene, wordt door het Cbp gezien als knelpunt.

4.3.4 Minderjarigen

Nouwt[267] bespreekt de bescherming van de persoonlijke levensfeer van minderjarigen op het internet. Deze auteur gaat daarbij met name in op de wijze waarop toestemming kan worden verkregen van de wettelijke vertegenwoordigers. Hij meent dat de privacy van kinderen op internet voldoende wordt beschermd door de Wbp, maar dat dit niettemin zou moeten worden meegenomen bij de evaluatie van de privacy-

[264] Art. 29 Werkgroep, 2006a; zie voor een toelichting Kohnstamm & Fontein 2006, p. 127-128.
[265] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
[266] Vgl. art. 8, onder d, en art. 16 jo. 23 Wbp.
[267] Nouwt 2004f, p. 52-58.

richtlijn die indertijd door de Commissie werd uitgevoerd. Verder dringt hij erop aan dat er zowel door verantwoordelijken als het Cbp vuistregels worden opgesteld. Verder kan met betrekking tot minderjarigen worden gewezen op de onduidelijklijkheden ten aanzien van het verkrijgen van toestemming van minderjarigen, al dan niet via de wettelijke vertegenwoordigers. De Artikel 29 Werkgroep[268] heeft aangegeven voornemens te zijn het toestemmingsbegrip, in het bijzonder in de relatie tot minderjarige kinderen, te gaan verduidelijken.

Als niet nader benoemd knelpunt wordt gewezen op de wijze waarop toestemming van minderjarigen kan worden verkregen.

4.4 Zelfregulering

4.4.1 Gedragscodes

De wetgever hecht veel betekenis aan zelfregulering en meer in het bijzonder gedragscodes, onder andere omdat deze worden geacht te voorzien in de concretisering en verdere invulling van het abstracte wettelijke normkader. Daarbij hebben gedragscodes, zoals alle vormen van zelfregulering, het voordeel dat deze eerder zullen worden aanvaard en nageleefd doordat ze zijn opgesteld door de verantwoordelijken zelf. Holvast[269] meent dat dit niet altijd zo werkt en uit kritiek op de wijze waarop uitvoering wordt gegeven aan de in artikel 25 van de wet geregelde goedkeuring van gedragscodes door het Cbp. In zijn interview met Cbp-voorzitter Kohnstamm stelt hij vast dat men in de praktijk niet erg tevreden is over de eigen ruimte die men in de praktijk heeft bij het opstellen van gedragscodes:

> 'De vinger van het Cbp wordt als te groot ervaren en eenmaal gemaakte codes verdwijnen in de kast om er nooit meer uit te worden gehaald. De flexibiliteit ontbreekt.'

Dergelijke kritische geluiden over de goedkeuringsbevoegdheid van het Cbp klinken ook door in het rapport van de Ambtelijke Commissie Toezicht II (ACT II). In gesprekken met de 'stakeholders' die deze commissie voerde werd onder meer gewezen op 'de soms dominante rol die het Cbp claimt in adviestrajecten'.[270] In de bijeenkomst met domeindeskundigen die in het kader van dit evaluatieonderzoek plaatsvond werd dit bevestigd, met name door de vertegenwoordigers uit de particuliere sector. In zijn reactie op de opmerking van Holvast reageert Kohnstamm op het verwijt van de 'te grote vinger' van het Cbp als volgt:

> 'Dat men klaagt over het gebrek aan eigen ruimte is universeel. Overal waar je zelfregulering ziet, klaagt de zichzelf regulerende partij over het feit dat er een te grote bemoeienis is. Ik ben geneigd 50% van de klachten overdreven te vinden, hetgeen niet wegneemt dat er ook bij zelfregulering een zekere rekkelijkheid moet zijn.'

Voor Kohnstamm is vooral van belang dat zelfregulering alleen een kans van slagen heeft als toezicht en handhaving fors worden ingezet. Andere auteurs wijzen op de tekortkomingen van zelfregulering en het ontbreken aan prikkels om deze op te stellen. Cuijpers[271] geeft aan dat het opstellen van gedragscodes een langdurig en tijdrovend, kostbaar proces is waar weinig concrete voordelen tegenover staan. In meer algemene termen wijst Nouwt[272] op een 'zelfreguleringstekort' waar het gaat om het gebruik van informatietechnologie. Een en ander speelt met name in de private sector, meer daarover in hoofdstuk 5.

---

[268] Art. 29 Werkgroep, Werkprogramma 2006-2007, WP120, 5 april 2006.
[269] Holvast 2005c, p. 114-119.
[270] ACT II 2004, p. 17.
[271] Cuijpers 2006.
[272] Nouwt 2005, p. 107-108.

Berkvens,[273] ten slotte, uit kritiek op het ontbreken van rechtsmiddelen als het gaat om de goedkeuring van Europese gedragscodes door de Artikel 29 Werkgroep. Dit raakt ook aan het functioneren van de wet omdat zo een gedragscode ook in Nederland werkt.

Waar het om gedragscodes wordt de invloed die het Cbp heeft op grond van zijn goedkeuringsbevoegheid gezien als knelpunt. Enkele auteurs wijzen erop dat het opstellen van gedragscodes een landurig, tijdrovend en kostbaar proces is waar weinig concrete voordelen tegenover staan.

4.4.2 Functionaris voor de gegevensbescherming

De Wbp heeft de functionaris voor de gegevensbescherming (FG) geïntroduceerd. Over het door de positie van de FG en het door hem of haar op te stellen verslag was ten tijde van de parlementaire behandeling van de wet als enige discussie. Indertijd is door de minister aangekondigd dat nog zal worden bezien hoe de praktijk zich op dit punt ontwikkelt en in hoeverre naar aanleiding daarvan nadere regels moeten worden gesteld.[274]

Over het instituut wordt door de functionarissen zelf geschreven, maar ook wel door anderen. Cbp-voorzitter Kohnstamm[275] meent dat de FG 'een onwaarschijnlijk relevant instrument' is. Wel acht hij het van belang dat de positie van de FG binnen de organisatie van de verantwoordelijke wordt versterkt. En daar ligt, zegt hij, toch wel een probleem:

> 'omdat sommigen onafhankelijk zijn en anderen in mindere mate. En dat hangt weer af van de opzet waarmee ze zijn aangesteld: zijn wij met een dergelijke aanstelling het probleem kwijt of proberen wij het probleem zo zuiver mogelijk te benaderen?'

Om de positie van de FG te versterken heeft het Cbp[276] het voorstel gedaan aan bemiddeling door een FG opschortende werking toe te kennen, zoals ook al het geval is bij bemiddeling door het Cbp. De Zeeuw,[277] vice-voorzitter van het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG), steunt dit voorstel. Verder gaat NGFG-voorzitter Titulaer.[278] Zij zegt het een positieve ontwikkeling te vinden dat functionarissen bij een aantal overheidsinstellingen verplicht worden gesteld en tekent daarbij aan dat het jammer is dat deze ontwikkeling zich in het bedrijfsleven nauwelijks voordoet – jammer, omdat het aanstellen van een interne toezichthouder:

> 'de zorg voor de kwaliteit van de gegevensverwerkingen in het algemeen ten goede komt'.

Zij zegt niet met zoveel woorden dat de FG ook in het bedrijfsleven verplicht moet worden gesteld, maar meent wel dat deze ontwikkeling bij de overheid bij het bedrijfsleven 'eenzelfde pendant' zou moeten oproepen. Bruin en Terstegge[279] zetten zich daartegen af. Volgens deze auteurs moet het aanstellen van een privacyfunctionaris (al dan niet zijnde een FG in de zin van de Wbp) gebeuren vanuit de overtuiging van de desbetreffende organisatie en niet zozeer vanuit een wettelijke verplichting. Dit sluit aan bij een eerdere opmerking van Prins[280] in haar beschouwing over de positie van de betrokkene. Zij stelt, overigens al toen er in Nederland nog geen of weinig ervaring was met de functionaris, dat de bijdrage die de interne toezichthouder kan bieden aan de positionering en de rol van betrokkenen wordt bepaald door 'de atmosfeer

---

[273] Berkvens 2003, p. 62.
[274] *Kamerstukken II* 1998-1999, 25 892, nr. 35.
[275] Holvast 2005c, p. 114-119.
[276] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
[277] De Zeeuw 2005.
[278] Titulaer 2006, p. 23-24.
[279] Bruin & Terstegge 2006, p. 185-186.
[280] Prins 1998, p. 11-14.

waarbinnen de functionaris moet opereren', en niet zozeer door de in de wet genoemde criteria van kennis, betrouwbaarheid en aanmelding bij het Cbp.

Holvast [281] maakt in een opiniërende tekst over de meldplicht een opmerking over de functionaris. Hij stelt dat voor betrokkenen die willen worden geïnformeerd over verwerkingen, de weg naar de functionaris in veel gevallen te onbegaanbaar is. In de bijeenkomst met domeindeskundigen die in het kader van dit onderzoek plaatsvond werd dit door de aanwezige FG's ontkend. Er werd op gewezen dat FG's in toenemende mate de bij hen gedane meldingen van gegevensverwerkingen via de websites van hun organisaties beschikbaar stellen. Omdat de betrokkene in de eerste plaats daar zal zoeken naar informatie over de hem of haar betreffende verwerking, wordt daarmee de transparantie van verwerkingen sterk verbeterd, waarbij wordt aangetekend dat het meldingsregister van het Cbp erg ontoegankelijk is. Vanuit de FG's werd er in de bijeenkomst ook op aangedrongen dat op de een of andere manier zou worden geformaliseerd dat het Cbp werkelijk op afstand blijft als er een FG is ingesteld binnen de organisatie van de verantwoordelijke. Verder werd erop aangedrongen dat zou worden vergemakkelijkt dat een derde partij, bijvoorbeeld een adviesbureau, de functie van FG zou kunnen vervullen. Dit zou kunnen worden gerealiseerd door niet te verlangen dat een FG een natuurlijke persoon is.

Het kunnen waarborgen van de onafhankelijkheid van de FG wordt gezien als knelpunt. Vanuit de organisatie van de FG's wordt erop aangedrongen dat in de private sector (al dan niet verplicht) meer FG's worden aangesteld. Andere auteurs menen dat dit niet zou moeten gebeuren vanuit een wettelijke verplichting. Over de bijdrage van de FG's aan de vergroting van de transparantie van verwerkingen zijn de meningen verdeeld. Vanuit FG's wordt wel aangedrongen op het formaliseren van de terughoudende rol van het Cbp als er een FG is aangesteld.

4.5 Transparantie en rechten van betrokkenen

Kennisnemingsrechten van betrokkenen

Al bij de evaluatie van de WPR bleek dat betrokkenen maar in beperkte mate gebruik maken of kunnen maken van kennisnemingsrechten.[282] Dit beeld lijkt, zo bleek uit de bijeenkomst met domeindeskundigen, niet veranderd, zij het dat er in bepaalde sectoren en om specifieke redenen wel veel gebruik wordt gemaakt van dit recht. Het gaat dan met name om de financiële sector, met name in het kader van procedures tegen de Dexia-bank. Verder blijkt ook dat in het kader van procedures over asielaanvragen nog al eens gebruik wordt gemaakt van het kennisnemingsrecht van de Wbp, waar vroeger gebruik werd gemaakt van de Wob. Of een en ander als knelpunt moet worden gezien is niet helemaal duidelijk. Uit de rechtspraak over de kennisnemingsrechten kan worden opgemaakt dat op dit moment er wel nog veel onduidelijkheid is over de reikwijdte en invulling van de kennisnemingsrechten. Ook de verhouding van kennisnemingsrechtenen regelingen in het Wetboek van rechtsvordering en de Wob blijkt vragen op te roepen.[283]

Een knelpunt waar het Cbp[284] in zijn brief met wijzigingsvoorstellen nog op wijst betreft de kosten die in rekening mogen worden gebracht voor het kennisnemen van röntgenfoto's. Om dit op te lossen zou het het Besluit Kostenvergoeding Wbp moeten worden aangepast.

---

[281] Holvast 2005d, p. 208-211.
[282] Prins e.a. 1995.
[283] Zie daarover: Van den Bergen 2005, p. 296-306; Berkvens 2005a, p. 119-121; Holvast, annotatie bij Rechtbank. Amsterdam 19 mei 2005 in *Computerrecht* 2005-6, p. 323-327; Rank & Haasjes 2005; Van Schoonhoven 2006a, p. 200-205; Zwenne & Webbink 2006, p. 2-8.
[284] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.

Uit onderzoek verricht in opdracht van de Europese Commissie blijkt dat verantwoordelijken in Nederland over het algemeen goed bekend zijn met de wettelijke kennisnemings- en verbeteringsrechten.[285] In het implementatierapport wordt opgemerkt dat de meerderheid van de verantwoordelijken geen moeite heeft om te voldoen aan kennisnemingsverzoeken van betrokkenen.[286]

Correctie en verzetsrechten van betrokkenen

In zijn brief aan de Minister van Justitie doet het Cbp[287] een aantal wijzigingsvoorstellen, waarvan enkele betrekking hebben op de rechten van betrokkenen. Een van deze betreft het ontbreken van de mogelijkheid voor de betrokkene om na te gaan of er is voldaan aan zijn verzoek om een verwerking terstond te beëindigen. Ook is daarmee onduidelijk wanneer de betrokkene eventueel gebruik kan maken van de rechtsmiddelen die de wet hem biedt als de verantwoordelijke niet voldoet aan zijn verzoek.

Een ander probleem waar het Cbp de minister op attendeert betreft het ontbreken van termijnen waarbinnen de verantwoordelijke op verzoek van de betrokkene bepaalde informatie moet verstrekken, namelijk waar het gaat om het op verzoek verstrekken van inlichtingen over een vrijgestelde melding of het kennisgeven van de correctie van gegevens. De wet noemt geen termijn waarbinnen de verantwoordelijke dit moet doen, met als gevolg dat onduidelijk is wanneer de betrokkene gebruik kan maken van de rechtsmiddelen die de wet biedt.

Op een specifiek gebied, namelijk dat van de kredietwaardigheidstoetsing, is het volgens Heuver[288] voor betrokkenen lastig om gebruik te maken van correctie- of aanvullingsrechten,

Waar het gaat om correctie en verzetsrechten signaleert het Cbp enkele omissies als gevolg waarvan het voor betrokkene lastig is om eventueel gebruik te maken van rechtsmiddelen.

Informatieplichten voor verantwoordelijken

Over de informatieplichten van de richtlijn, in de Wbp geïmplementeerd in de artikelen 33 en 34, merkt de Commissie in haar Implementatierapport op veel knelpunten voortkomen uit de verschillen in de nationale wetgeving, maar ook het gevolg is van uiteenlopende interpretaties door toezichthouders.:

> 'The implementation of Articles 10 and 11 of the Directive [betreffende de informatieplichten] showed a number of divergences. To some extent this is the result of incorrect implementation, for instance when a law stipulates that additional information must always be provided to the data subject, irrespective of the necessity test the Directive foresees, but also stems from divergent interpretation and practice by supervisory authorities. Submissions stressed the difficulties for multinational companies operating on a pan-European level that arise from these divergences'.

Dit is uiteraard vooral een probleem voor verantwoordelijken die gegevens verwerken in meerdere lidstaten, zoals met name multinationale ondernemingen of in de publieke sector het Ministerie van buitenlandse Zaken.[289]

Een aantal auteurs, zoals Merkus,[290] maakt opmerkingen over het niet voldoen of het niet kunnen voldoen aan de informatieplichten van de Wbp, soms als een opmerking terzijde maar soms ook als aanduiding van

[285] EOS Gallup 2003, p. 30.
[286] Implementatierapport, p. 9.
[287] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
[288] Heuver 2003, p. 55-61.
[289] Dit bleek in de bijeenkomst met domeindeskundigen die in het kader van dit onderzoek plaatsvond.
[290] Merkus 2002, p. 14-18.

een serieus knelpunt. Dubbeld[291] sluit haar bespreking van medische websites, door haar aangeduid als telemedicine websites, af met de conclusie dat het informeren van betrokkenen op deze websites veel te wensen overlaat. Het Cbp[292] erkent dat de interpretatie en uitleg van de voor de informatieplichten relevante open normen aanleiding geeft tot veel onzekerheid, meer in het bijzonder waar het gaat om de verplichting om nadere informatie te verstrekken om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. Bij de oplossing van dit probleem ziet het Cbp een rol voor zichzelf. De toezichthouder geeft aan dat:

> '[e]r zal gewerkt worden aan een standaardisering van de informatieplicht. Dit kan ofwel betekenen dat de huidige open normen nader worden ingevuld, ofwel dat aanpassing van de Wbp vereist is.'

Cbp-voorzitter Kohnstamm[293] gaat in een interview met Holvast niet zozeer in op de interpretatie van de desbetreffende begrippen. Wel geeft hij aan ervoor te willen gaan zorgen dat verantwoordelijken beter, sneller en effectiever aan de informatieplichten voldoen en denkt daarbij aan handhaving en zelfregulering. Ook denkt hij dat de FG's daar in zijn of haar jaarverslag aandacht aan zouden moeten geven.

Daarnaast lijkt er ook sprake te zijn van knelpunten met betrekking tot de bekendheid of bewustwording ('awareness')[294] ten aanzien van de informatieplichten. Uit onderzoekverricht in opdracht van de Europese Commissie blijkt dat in Nederland betrekkelijk veel verantwoordelijken menen dat zij niet zijn gehouden om betrokkenen te informeren over de doeleinden waarvoor zij persoonsgegevens verwerken.[295] Uit specief op Nederland gericht onderzoek blijkt dat betrokkenen het gevoel hebben maar weinig inzicht te hebben in de mate waarin organisaties omgaan met persoonsgegevens. Uit hetzelfde onderzoek blijkt ook dat betrokkenen wel veel belang hechten aan dit inzicht.[296]

De Commissie ziet met het Cbp en enkele auteurs knelpunten waar het gaat om de interpretatie van de voor de informatieplichten relevante begrippen. De bekendheid of bewustwording ('awareness') met informatieplichten blijkt zowel bij verantwoordelijken als betrokkenen beperkt. Het CBP ziet handhaving en zelfregulering als middelen om knelpunten met betrekking tot de naleving van informatieplichten te verhelpen.

Meldplicht

In het voorgaande is al aangegeven dat de de wetgever ervoor heeft gekozen om bij de meldplicht uit te gaan van de systematiek, waarbij als algemene regel in beginsel alle verwerkingen moeten worden gemeld, tenzij er in het Vrijstellingsbesluit voor een bepaalde verwerking een vrijstelling is opgenomen. Dit wordt wel aangeduid als de 'genormeerde vrijstelling'. Blok[297] stelt deze systematiek op principiële reden ter discussie en stelt zich op het standpunt dat deze de overzichtelijkheid van het rechtsgebied niet heeft bevorderd. Hij doet het voorstel om de meldplicht te beperken tot de gegevensverwerkingen die buiten de betrokkenen om plaatsvinden. Holvast[298] sluit zich aan bij deze kritiek op de meldplicht. In een opiniërende tekst onder de veelzeggende titel 'De aanmeldplicht, een overbodige bepaling?' stelt hij vast dat de meldplicht niet bijdraagt aan de transparantie van verwerkingen, zoals de wetgever beoogt, en evenmin bij-

[291] Dubbeld 2006, p. 132-136.
[292] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[293] Holvast 2005c, p. 114-119.
[294] In meer algemene zin had de Raad van State al in zijn advies over het wetsvoorstel gevraagd om specifieke aandacht voor een tijdige en uitgebreide voorlichting over de implicaties van de invoering van de wet; *Kamerstukken II* 1997–1998, 25 892, A p. 1.
[295] EOS Gallup 2003, p. 59.
[296] Schildmeijer, Samson & Koot 2005, p. 10-11 en 19.
[297] Blok 2002, p. 318.
[298] Holvast 2005d, p. 208-211.

draagt aan de privacybewustwording van verantwoordelijke, wat het Cbp als extra doelstelling ziet. En daarbij leidt de meldplicht volgens hem tot administratieve lasten. Een en ander komt ook naar voren in het rapport van ACT II.[299] Daar blijkt dat er vraagtekens zijn bij het nut en de toegevoegde waarde van de meldplicht. De in dit rapport geïnterviewde 'stakeholders' vragen zich af:

> 'wat het nut en de noodzaak is van deze melding. Ondanks het grote aantal vrijstellingen levert deze melding voor bedrijven administratieve lasten op. Bovendien zijn veel bedrijven bang dat zij door middel van die melding concurrentiegevoelige informatie prijsgeven. Stakeholders vragen zich af wat het Cbp nu echt doet met de meldingen, welk doel het dient en wat het Cbp er mee wil bereiken.'

Evenals VNO-NCW[300] is Holvast kritisch over de door het Cbp[301] en ook wel door ander auteurs, zoals Essen,[302] voorgestelde oplossingen, te weten: het uitbreiden van het aantal vrijstellingen. Dat is volgens Holvast 'slechts een stap in de goede richting' maar leidt niet tot een echte verbetering. Een oplossing waar hij wel voor voelt is de eveneens door VNO-NCW voorgestelde genormeerde meldplicht.[303] Meer hierover ook in paragraaf 4.7 over uitvoeringskosten en in hoofdstuk 5 over de private sector.

Zoals in het voorgaande besproken doet het Cbp[304] in zijn brief aan de Minister een voorstel voor de oplossing van een deel van dit probleem, namelijk waar het toepassing van de meldplicht betreft op verantwoordelijken die in verschillende lidstaten zijn gevestigd. Het Cbp stelt voor dat er een standaard meldformulier wordt ontwikkeld waarmee de verwerkingen in de verschillende lidstaten eenmalig kan melden.

De te ruime werking van de meldplicht wordt algemeen gezien als een knelpunt. Over de oplossing daarvan verschilt men van mening. Ook zijn er vraagtekens over de bijdrage die de meldingen leveren aan de beoogde transparantie.

4.6 Toezicht en rechtsbescherming

4.6.1 Toezicht

Middelen en bevoegdheden, effectiviteit

In het Implementatierapport gaat de Commissie[305] in op de mogelijkheden om naleving van de privacywetgeving te controleren en te handhaven. De Commissie stelt zich op het standpunt dat nationale privacytoezichthouders over te weinig middelen beschikken en dat er maar weinig aandacht is voor handhaving:

> 'An under-resourced enforcement effort and supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority'

Discussies over de omvang van de toezichthoudende bevoegdheden van het Cbp waren ten tijde van de parlementaire behandeling van de Wbp aanleiding voor de minster om aan te kondigen dat daaraan in de evaluatie van de wet aandacht wordt besteed.[306] Of er inderdaad sprake is van te weinig of teveel handhavingsbevoegdheden blijkt in beperkte mate uit de literatuur. Vaak gaat het om opmerkingen in de marge

[299] ACT II 2004, p. 14.
[300] NVO-NCW, Brief d.d. 15 december 2004, kenm. 04/15.098/Gf/CV.227.
[301] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[302] van Essen 2003, p. 360-367.
[303] Zie ook ACT II 2004, p. 15 en 31.
[304] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[305] Implementatierapport, p. 12-13.
[306] *Kamerstukken II* 1998-1999, 25 892, nr. 8, p. 31.

of met een meer terloops karakter. Een voorbeeld is een persbericht dat dateert van net na de invoering van de Wbp, waarin het E-Commerce Platform[307] aangeeft dat de wet onvoldoende waarborgen biedt voor effectieve zelfregulering, hetgeen onder andere wordt verklaard door een te verbrokkeld toezicht. In een korte opiniërende tekst over de opheffing van de digitale burgerrechtenbeschermers Bits of Freedom spreekt Schmidt[308] over 'het verontrustende papieren-tijger-gehalte van ons Cbp', wat erop zou kunnen duiden dat de toezichthouder volgens deze auteur te weinig bevoegdheden heeft. In een publicatie over de internationale doorgifte van persoonsgegevens stelt De Vries[309] aan de orde dat er een scheefgroei dreigt te ontstaan tussen, enerzijds, de verantwoordelijken die de wet naleven en daardoor te maken krijgen met de toezichthouder, en anderzijds, degenen die zich verschuilen achter de onduidelijkheden van de wet en die vooralsnog de dans lijken te ontspringen.

In enkele brieven[310] die het Cbp in het najaar van 2002 stuurde naar de minister en de Vaste Commissie voor Justitie spreekt de toezichthouder de zorg uit over de voorgenomen bevriezing van het budget van het Cbp in de Justitie-begroting. Als gevolg daarvan zou de handhaving van de wet 'in een beslissende fase' worden verstoord. Enkele jaren later wordt Cbp-voorzitter Kohnstamm op de voorpagina van de Staatscourant aangehaald waar hij aangeeft dat hij graag wat meer bevoegdheden voor zijn college zou zien. Behalve meer bevoegdheden om boetes op te leggen aan organisaties die de wet niet naleven, zou hij ook willen dat het Cbp de mogelijkheid had om wetten ter vernietiging voor te dragen bij de Hoge Raad of het Europees Hof van Justitie.[311]

Uit onderzoek verricht in opdracht van de Europese Commissie blijkt dat niet-naleving van de privaywetgeving in verband wordt gebracht met een gebrek aan bekendheid of bewustwording bij verantwoordelijken, dan met te weinig bevoegdheden van de toezichthouder.[312] In dat verband kan ook worden gewezen op een ander onderzoek, waaruit blijkt dat de bekendheid van het Cbp gering is en dat maar weinig betrokkenen aangegeven zich tot de toezichthouder te zullen wenden als zij problemen zouden hebben met de bescherming van persoonsgegevens.[313] In een verslag over de jaarlijkse internationale conferentie van toezichthouders persoonsgegevens lijkt Holvast[314] een wat ironische toon aan te slaan als het gaat over de noodzaak van toezichthouders en de veelheid van bevoegdheden waarover deze beschikken.

Van der Horst[315] wijst er in zijn bijdrage aan het handboek *Privacyregulering in theorie en praktijk* op dat handhaving van de naleving van de wet problematisch is omdat de wet door zijn definities en casuïstiek een enorme reikwijdte heeft. Dit betekent dat de er een erg groot 'controleapparaat' moet zijn om de naleving waar nodig af te dwingen. In de praktijk zal dat volgens deze auteur niet haalbaar zijn, zeker als daarbij in aanmerking wordt genomen dat de 'pakkans' gering is. Of hij daarmee doelt op de controlemiddelen van de verantwoordelijke zelf of de bevoegdheden van de toezichthouder, is niet helemaal duidelijk. Wel geeft deze auteur aan dat hij 'een praktische benadering' voorstaat om ervoor te zorgen dat privacybescherming hoog op de prioriteitenlijst van organisaties staat. Om ervoor te zorgen dat de Wbp meer serieus wordt genomen door verantwoordelijken stelt Nouwt voor om overtredingen van de wet meer strafrechtelijk te sanctioneren. Hij stelt dat het rechtsbelang dat in het geding is – volgens hem de vertrouwelijkheid van

---

307 Persbericht E-commerce Platform 13 november 2001, aangehaald in *P&I* 2002-1, p. 34-35; het desbetreffende rapport waaruit dit zou blijken is niet meer beschikbaar via openbare bronnen.
308 Schmidt 2006, p. 245.
309 De Vries 2006, p. 265-267.
310 Vgl. Brief van de vzr van het Cbp aan de Vaste Commissie voor Justitie d.d. 22 oktober 2002; Brieven van de vzr. van het Cbp aan de Minister van Justitie d.d. 26 augustus 2002 en 25 september 2002, kenm. 2002-F2207.
311 'Investeren nodig in goede omgang persoonsgegevens', *Stcrt.* 12 juli 2006.
312 EOS Gallup 2003, p. 70.
313 Schildmeijer, Samsons & Koot 2005, p. 21.
314 Holvast 2002a, p. 260-261.
315 Van der Horst 2002, p. 113.

persoonsgegevens en daarmee het vertrouwen van burgers in de overheid – ervoor pleit het strafrechtelijk sluitstuk van de wet uit te breiden.[316] Deze auteur ziet dit als verbeterpunt voor de naleving van de wet.

Over de vraag of het Cbp voldoende of te weinig bevoegdheden heeft wordt verschillend gedacht. In de literatuur wordt gewezen op knelpunten met betrekking tot de naleving van de wet, die ook kunnen worden geduid als knelpunten op het gebied van de handhaving. Een enkele auteur pleit voor meer aandacht voor de strafrechtelijke handhaving van de wet.

Onafhankelijkheid Cbp

In het Implementatierapport merkt de Commissie op dat in sommige gevallen – welke gevallen dat zijn blijft in het midden – de onafhankelijkheid van toezichthouders te wensen overlaat. Dat toezichthouders over te weinig middelen en bevoegdheden beschikken is volgens haar wel duidelijk.

> 'The independence of some supervisory authorities is exemplary, whilst in other countries it is clearly insufficient. On the other hand, all the supervisory authorities lack the necessary resources and some also the necessary powers to ensure effective implementation of data protection legislation.'

Over de onafhankelijkheid van het Cbp blijken uit de literatuur geen echte knelpunten. Wel gaat Ambtelijk Commissie Toezicht II[317] (ACT II) in op de bestuurlijke verhoudingen tussen het Cbp en de Minister van Justitie. De commissie stelt vast dat de minister, gelet op de onafhankelijkheid van het Cbp, geen inhoudelijke aansturende rol heeft richting het Cbp en alleen verantwoordelijk is voor de financiering en de apparaatzorg. Onder verwijzing naar de kabinetsstandpunt over het advies Vertrouwen in onafhankelijkheid[318] wijst de commissie erop dat de minister wel moet beschikken over een algemene aanwijzingsbevoegdheid, maar dat daar in de inhoudelijke sfeer geen invulling aan wordt gegeven. In dat verband wijst de commissie op het belang dat de beleidskaders worden bepaald door de minister, niet door de toezichthouder zelf:

> 'Goed toezichtbeleid geeft aan wat het doel van het toezicht is, met welke frequentie en diepgang het wordt uitgeoefend, welke prioriteiten in het toezicht gesteld worden en welke risico's het voorgestelde toezicht zouden kunnen bevatten (de beleidskaders). Van belang is daarbij dat door een adequate invulling van de toezichtsfunctie kritische factoren in het beleidsproces kenbaar en beheersbaar worden. Niet de toezichthouder zelf, maar de beleidskaders van de Minister en de wet- en regelgeving bepalen waarop toezicht wordt gehouden.'

Voor de commissie is dit een belangrijk aandachtspunt in het toezichtarrangement. De commissie doet dan ook de aanbeveling dit te betrekken in de evaluatie van de Wbp en in dat kader te bezien in hoeverre de minister zijn beleidskaders beter kenbaar kan maken.[319]

Met betrekking tot de onafhankelijkheid van het Cbp wijst de Ambtelijke Commissie Toezicht II op het aandachtspunt dat inhoudelijk geen invulling wordt gegeven aan de algemene aanwijzingsbevoegdheid van de minister.

---

[316] Over de strafrechtelijke sancties en bestuurlijke boetes heeft het Cbp in zijn brief d.d. 12 juli 2005 met wijzigingsvoorstellen aangegeven dat deze niet in de pas lopen. Zo kan de toezichthouder bij overtreding van de meldplicht een bestuurlijke boete opleggen van ten hoogste 4500 euro, terwijl als misdrijf gekwalificeerde strafbare feit van opzettelijk niet melden wordt bedreigd met gevangenisstraf of een geldboete van 2250 euro. Deze situatie acht het Cbp niet wenselijk, wat zou kunnen duiden op een knelpunt.

[317] ACT II 2004 p. 9-15.

[318] *Kamerstukken II* 2000-2001, 27 831, nr. 1, p. 16.

[319] Zie ook *Kamerstukken II* 2005/06, 29 800, nr. 163.

Publicatiebeleid cq. publieke schandpaal ('naming and shaming')

Het publiceren van namen van overtreders van de Wbp wordt door het Cbp wel gezien als een:

> 'effectief middel (…) dat toezichthouders ter beschikking staat om naleving te bevorderen.'[320]

Voor en tijdens de parlementaire behandeling van de Wbp was er discussie over het gebruik van dit middel, dat ook wel wordt aangeduid als de 'publieke schandpaal-methode' of 'naming and shaming'.[321] Over de wijze waarop dit middel wordt gebruikt heeft het Cbp regels vastgelegd in beleidsregels,[322] waarin staat dat de toezichthouder zijn oordelen openbaar maakt in de gevallen waarin hij van mening is dat daarmee een maatschappelijk belang kan worden gediend. Als het gaat om overheidsinstelling wordt bekend gemaakt om welke instelling het gaat – dit in aansluiting op het publicatiebeleid van de Nationale Ombudsman. Als het gaat om een particuliere organisatie wordt een meer terughoudend beleid gevoerd en wordt in de regel een geanonimiseerd oordeel gepubliceerd. In een aantal gevallen wordt toch overgegaan tot het bekendmaken van een particuliere organisatie, namelijk (i) als bij derden is reeds bekend is dat er een zaak over de organisatie is voorgelegd, (ii) als er sprake is van een groot aantal klachten of belanghebbenden bij de onderzochte verwerking van persoonsgegevens, en (iii) als de betrokken organisatie zelf publiciteit heeft gezocht over de (voorgenomen) verwerking van persoonsgegevens.

Een blik op de website van het Cbp leert dat de afgelopen jaren vooral de namen van grote particuliere organisaties zijn bekendgemaakt. Denk aan: Dexia Bank, KPN, ING en Postbank. Over dit 'actieve publicatiebeleid' zijn de meningen nog steeds verdeeld. Uit een voorpagina-bericht in de Staatscourant lijkt te kunnen worden opgemaakt dat Cbp-voorzitter Kohnstamm[323] voorstaat dat het Cbp verplicht zou worden om de namen te noemen van de verantwoordelijke die onderwerp is van een door de toezichthouder uitgevoerd onderzoek. Op dit moment zou dat niet kunnen, omdat de toezichthouder aansprakelijk zou kunnen worden gesteld als een bedrijf daardoor reputatieschade oploopt.[324] Vanuit vooral het bedrijfsleven[325] is er nog steeds kritiek op een dergelijke methode van handhaving of toezichthouden, zij het dat deze kritiek meer algemeen gericht is tegen naming and shaming en niet zozeer tegen het gebruik daarvan door het Cbp. Meer hierover in hoofdstuk 5.

Over 'naming and shaming' of een 'actief publicatiebeleid' zijn de meningen verdeeld. Waar het gaat om het bekendmaken van de namen van particuliere organisaties voert het Cbp een terughoudend beleid. Vanuit het Cbp wordt gedacht aan een wettelijk verplicht verdergaand publicatiebeleid. Vanuit vooral het bedrijfsleven is daar kritiek op.

4.6.2 Rechtsbescherming

Weinig betekenis van de Wbp in procedures

In de literatuur wordt door verschillende auteurs teleurstelling uitgesproken over de beperkte betekenis van de Wbp in de gerechtelijke procedures. Gutwirth & De Hert[326] maken zich, ter illustratie van wat zij

---

320 Cbp, Publicatie van persoonsgegevens op internet. Een verkenning, 17 mei 2006, p. 28.
321 Vgl. Kuitenbrouwer 2002, p. 53-54 en de aldaar genoemde bronnen, o.a. Van de Pol 1998b, p. 135; idem Van de Pol 1998a, p. 15-19; *Handelingen II* 17 november 1999, p. 23-1696, 23-1697 en 23-1709.
322 Uitgangspunten en beleidsregels werkwijze Cbp, *Stcrt.* 2004, 190.
323 'Investeren nodig in goede omgang persoonsgegevens', *Stcrt.* 12 juli 2006.
324 Vgl. Rechtbank Den Haag, 3 maart 2004, *LJN* AO4880 waarin de rechtbank oordeelde dat NMa, niet onrechtmatig had gehandeld door de publicatie van een persbericht over gedragingen van fietsfabrikanten in strijd met de Mededinginswet, hoewel er is wel sprake was van 'schoonheidsfouten'.
325 Vgl 'Supermarkten tegen openbaarheid controle', Financieel dagblad 10 juli 2006.
326 De Hert & Gutwirth 2004, p. 587-631.

onder andere zien als problemen met privacywetgeving, druk over de kantonrechters die geen acht slaan op de vele, maar onduidelijke adviezen van het Cbp over de controle door werkgevers van e-mailverkeer van werknemers:

> 'In Nederland treft ons dan de ogenschijnlijk drukke activiteit van het Cbp rond controle door de werkgever van e-mails, maar de adviezen van het Cbp worden door geen enkele arbeidsrechter gevolgd of gebruikt en in die adviezen wordt ten onrechte een onduidelijk antwoord gegeven op de essentiële vraag 'of een werkgever zonder enige individuele of collectieve kennisgeving e-mails mag controleren.'

Hoewel uit deze opmerking ook kritiek op de toezichthouder doorklinkt,[327] lijkt dit ook gericht tegen de rechters of misschien wel de rechtsbijstandverleners die kennelijk nog niet voldoende in staat zijn om de Wbp te betrekken in procedures. In een beschouwing met de sprekende titel 'Het verborgen bestaan van de Wet bescherming persoonsgegevens' merken ook Kolk & Verbruggen[328] op dat arbeidsrechters weinig doen met de Wbp. Ook de FNV[329] noemt dit knelpunt. Overkleeft-Verburg uit in dit verband verschillende malen kritiek op de Afdeling bestuursrechtspraak van de Raad van State vanwege een ondeugdelijke juridische toetsing aan de Wbp en gemiste kansen als het gaat om de interpretatie door de Afdeling van open geformuleerde bepalingen uit de Wbp[330] Andere auteurs wijzen erop dat overtreding van de Wbp niet ertoe leidt dat de aldus door de werkgever verkregen informatie buiten de ontslagprocedure wordt gehouden, maar vooral betekenis heeft bij het bepalen van de hoogte van de ontslagvergoeding.[331]

Elders[332] wordt wel gewezen op de omstandigheid dat er, mede in het licht van de grote reikwijdte van de wet, betrekkelijk weinig wordt geprocedeerd over de toepassing en werking van de Wbp.[333] Hoewel dit ook zou kunnen worden opgevat als een aanwijzing dat de wet kennelijk voldoende duidelijk is en/of een groot conflictoplossend vermogen heeft, wordt dit toch vooral gezien als een probleem omdat daardoor de open normen en vage begrippen in de wet maar in beperkte mate nader worden ingevuld en geconcretiseerd. Voorzover het gaat om het kennisnemingsrecht is dit beeld sinds kort aan het veranderen door de zgn. Dexia-jurisprudentie en ook wel andere uitspraken.[334] Over de reikwijdte van dat kennisnemingsrecht en in het verlengde daaraan de uitleg van het bestandsbegrip wordt sinds kort veel geprocedeerd. Uit de publicaties over deze rechtspraak, onder ander van Van den Bergen,[335] Berkvens,[336] Holvast,[337] Rank & Haasjes,[338] Van Schoonhoven[339] en Zwenne & Webbink,[340] blijkt dat een aantal onduidelijkheden van de

---

[327] Vgl. De Hert 2002, p. 26-30.
[328] Kolk en Verbruggen 2002, p. 3-10.
[329] FNV 2003.
[330] ABRvS 11 augustus 2004, *JB* 2004/325, m.nt. G. Overkleeft-Verburg; zie ook: ABRvS 12 mei 2004, *JB* 2004/251, m.nt. G. Overkleeft-Verburg; ABRvS 12 juli 2006, m.nt. G. Overkleeft-Verburg; ABRvS 7 december 2005, AU7614, *JB* 2006, 50 m.nt. G. Overkleeft-Verburg.
[331] Jager 2003, p. 10-16; Even 2003, p. 37-39; L. Bijlsma & T.C.B. Homan 2003, p. 164-167; Lacevic & Zondag 2004, p. 91-98.
[332] Onder andere door de deelnemers aan de expertbijeenkomst die in het kader van dit evaluatie onderzoek plaatsvond op 29 augustus 2006.
[333] Een indicatie van het aantal procedures waarin de Wbp een rol speelde kan worden ontleend aan de uitspraken gepubliceerd via www.rechtspraak.nl: de zoekterm 'Wbp' geeft als resultaat ca. 120 uitspraken over de wet (en iets meer dan 40 uitspraken van de Centrale Raad van Beroep waarbij de Raadskamer WBP van de Pensioen- en Uitkeringsraad partij was).
[334] Bijv. Rechtbank Den Bosch 31 maart 2004, *LJN* AT3148; Rechtbank Den Haag 7 april 2004, *LJN* AO8756; Rechtbank Arnhem 5 oktober 2006, *LJN* AX1994.
[335] Van den Bergen 2005, p. 296-306.
[336] Berkvens 2005a, p. 119-121.
[337] Holvast 2005a, p. 323-327.
[338] Rank & Haasjes 2005.
[339] Van Schoonhoven 2006a, p. 200-205.
[340] Zwenne & Webbink 2006, p. 2-8.

wet wordt opgehelderd, maar veel ook nog niet. Over de uitleg van begrippen als 'onevenredige inspanning' en 'bestand', en over de betekenis van een gedragscode is nog geen eenduidige jurisprudentie uitgekristalliseerd.

Er wordt betrekkelijk weinig geprocedeerd over de toepassing en werking van de Wbp. Daardoor blijft onzekerheid bestaan over de invulling en concretisering van veel open normen in de wet. Op enkele deelonderwerpen, zoals het kennisnemingsrecht is dit beeld aan het veranderen en ontstaat er thans wel jurisprudentie waarin relevante begrippen worden geconcretiseerd

Verschillende procedures en inconsistenties

Schilder[341] wijst op de verschillen van procedurele aard als het gaat om de rechtsgangen die betrokkenen hebben wanneer zij tegen een bestuursorgaan of een bedrijf of particulier procederen over de wet: als het gaat om een procedure tegen een bestuursorgaan zal er eerst (mogelijk)[342] een bezwaarprocedure moeten worden doorlopen. Hij meent dat deze verschillen nog steeds moeilijk te verdedigen zijn en dat het bezwaar bestaat dat verschillende rechters rechtspraak vormen op een en hetzelfde gebied. Dit kan volgens deze auteur in de praktijk niet alleen tot verwarring leiden, maar ook tot rechtsongelijkheid. Ook meent hij dat het tweeledige systeem van rechtsbescherming voorbijgaat aan de complexe materie van het zelfstandig schadebesluit uit het bestuursrecht. En daarbij is forumshopping (d.w.z. het kiezen voor een rechterlijke instantie waarvan men het meest verwacht) niet uitgesloten. De auteur stelt dat de kans reëel lijkt dat de wetgever deze vanuit rechtszekerheid onwenselijke situatie niet op zijn beloop zal kunnen laten en uiteindelijk de bestuursrechtelijke rechtsgang als de exclusieve rechtsgang aanwijst ten aanzien van zelfstandige schadebesluiten. Hij spreekt tevens de gedachte uit dat mede gelet op deze zelfstandige schadebesluiten, de burgerlijke rechter in privacygeschillen weer zijn oude WPR-taken terugkrijgt.[343]

Ook Overkleeft-Verburg heeft kritiek op de verschillende procedures. De gedeeltelijke overlap in rechtsmacht tussen het College van Beroep voor het bedrijfsleven en de Afdeling bestuursrechtspraak wringt en leidt tot onbevredigende resultaten.[344] Over de rechtsmachtverdeling tussen de Afdeling bestuursrechtspraak en de Centrale Raad van Beroep stelt de auteur:

> 'Aannemelijk is dat de huidige rechtsmachtverdeling niet zozeer het product is van een uitdrukkelijke beslissing van de wetgever bij de totstandkoming van de Wbp, maar van een omissie om in de aanpassingswet ook de bijlage in de Beroepswet aan te vullen.'[345]

Daarnaast wijzen Cuijpers[346] en Terstegge[347] erop dat het gedifferentieerde systeem van toezicht tot nadelige gevolgen kan leiden, zoals forumshopping, inconsistenties in rechterlijke competenties en afbreuk van rechtseenheid.

Aan het systeem van verschillende bestuurs- en civielrechtelijke procedures zijn volgens enkele auteur nadelen verbonden, zoals forumshopping en in rechterlijke competenties en afbreuk van rechtseenheid.

---

341 Schilder 2002, p. 117-135.
342 Art. 7.1a Awb biedt sinds 1 september 2004 de mogelijkheid van rechtstreeks beroep.
343 Schilder 2002, p. 124.
344 CBB, 9 maart 2005, AT2597, zaaknr. AWB 04/58, m.nt. G. Overkleeft-Verburg.
345 ABRvS 12 januari 2005, *JB* 2005, 75 m.nt. G. Overkleeft-Verburg.
346 Cuijpers 2004, p. 340-350.
347 Terstegge 2000, p. 243-251.

4.7 Internationale gegevensdoorgifte

Doorgiftevergunning

Van knelpunten met betrekking tot de internationale doorgifte is, zo blijkt uit de literatuur voornamelijk sprake in de private sector. De gesignaleerde knelpunten zien met nameop de vergunningaanvragen die gegevensexporteurs moeten doen bij het Cbp als zij gebruik maken van de door de Commissie goedgekeurde model contracten ('standard clauses'). In 2003 merkt Cbp daarover op dat het aantal vergunningaanvragen voor internationale doorgifte van persoonsgegevens sterk achter blijft bij de verwachtingen, en ook dat er:

> 'een spanning lijkt te bestaan tussen de praktijk van doorgifte van persoonsgegevens en de regels die hierop van toepassing zijn.'[348]

In het Implementatierapport geeft de Commissie aan dit ook zo te zien. Op basis van het geringe aantal meldingen van gegevensdoorgiften (o.g.v. art. 26, tweede lid, van de richtlijn) vermoedt de Commissie dat:

> "many unauthorised and possibly illegal transfers [...] to destinations or recipients not guaranteeing adequate protection"

Tegelijkertijd wijs de Commissie op het probleem dat sommige lidstaten (waaronder Nederland) ook een doorgiftevergunning verlangen als er gebruik is gemaakt van de door de Commissie goedgekeurde standaardcontracten en er geen twijfel zou moeten zijn over de rechtmatigheid van de doorgifte. In dergelijke gevallen staat de richtlijn weliswaar toe dat de lidstaten een melding verlangen van deze doorgiften, maar dat is niet hetzelfde als een vergunning:

> 'Whilst the data protection authority may legitimately require the notification of these transfers, there is no need to authorize these transfers because they are already authorised by Community law.'[349]

De Vries[350] spreekt in dat verband over een 'in de praktijk als ergerniswekkend ervaren, administratieve last'. Zwenne[351] heeft het over overbodige en doorgeschoten regelgeving. Hij wijst erop dat het verkrijgen van deze doorgiftevergunning een formaliteit betreft waarvoor in de praktijk niettemin al gauw een wachttijd geldt van tenminste vier weken. Merkus[352] dringt aan op het door de minister afgeven van een algemene vergunning voor doorgiften gebaseerd op de modelovereenkomsten. Eind 2004 geeft ook het Cbp[353] aan dat het de vergunning in deze situatie onnodig vindt. Het verzoekt de minister om een vrijstelling voor de vergunningplicht te verlenen als de verantwoordelijke gebruik maakt van de standaardcontracten. Deze vrijstelling is evenwel nog niet verleend. Meer hierover in het hoofdstuk over de particuliere sector.

Waar het gaat om internationale doorgifte wordt vooral het vergunningvereiste dat ook geldt als gebruik wordt gemaakt van de modelcontracten ervaren als een knelpunt.

Doorgiftebegrip en uitzonderingen

Over het begrip 'doorgifte' en de uitzonderingen op het doorgifteverbod maakt Thijssen[354] een paar opmerkingen. Zij wijst erop dat het Europees Hof van Justitie in het Lindqvist-arrest een uitzondering heeft geformuleerd op de doorgifteregels, namelijk door beschikbaarstelling van gegevens op een webpagina

[348] Cbp, Mededeling, 12 juni 2003.
[349] Implementatierapport, p. 18.
[350] De Vries 2006, p. 265-267.
[351] Zwenne 2003, p. 322-323.
[352] Merkus 2004, p. 12-16.
[353] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[354] Thijssen 2005, p. 110-113.

niet te onder het begrip 'doorgifte' te begrijpen. Eenzelfde benadering staat zij voor waar het gaat het probleem dat doorgifte van de ene in de EU gesitueerde vestiging naar de andere buiten de unie gesitueerde vestiging van dezelfde verantwoordelijke niet goed lijkt te kunnen worden vormgegeven door de modelovereenkomsten – omdat de verantwoordelijke dan met zichzelf een overeenkomst zou aangaan. Als oplossing voor dit probleem stelt zij voor dergelijke doorgiften niet te kwalificeren als doorgifte in de zin van artikel 76 Wbp.

De Vries[355] wijst op de onduidelijkheden over de voor doorgifte relevante begrippen en uitzonderingen, die ook al door zowel de Commissie[356] als het Cbp[357] waren geconstateerd. Omdat de doorgiftevergunning wordt gezien als een 'ergerniswekkende administratieve last' is het volgens De Vries begrijpelijk dat verantwoordelijken de uitzonderingen op het doorgifteverbod ruim te interpreteren. Daarbij merkt zij op dat het Cbp zich niet meer uitlaat over de invulling van deze uitzonderingen. Om deze reden zou dit in het kader van de evaluatie van de wet moeten worden geanalyseerd.

Ook de Artikel 29 Werkgroep[358] onderkent dat de interpretatie en uitleg van de voor doorgifte relevante begrippen aanleiding geeft tot knelpunten. Om deze te verhelpen doet de werkgroep een aantal aanbevelingen die de verantwoordelijken ertoe moeten aanzetten in zoveel mogelijk situaties de vereiste passende bescherming te bieden. Ook geeft de werkgroep aanwijzingen voor de interpretatie van de in de richtlijn gedefinieerde uitzonderingen op het doorgifteverbod, waarbij hij in het bijzonder de begrippen 'toestemming' en 'uitvoering van een overeenkomst' verder uitwerkt – dit omdat in de praktijk het meest van deze uitzonderingen gebruik zou worden gemaakt. Anders dan de zo even genoemde auteurs kiest de werkgroep voor het uitgangspunt dat deze uitzonderingen restrictief moeten worden geïnterpreteerd. In dat verband wijst de werkgroep op het Verdrag inzake gegevensbescherming, met name het aanvullend protocol daarbij. Ook verwijst de werkgroep naar het Europees Hof voor de Rechten van de Mens, dat mensenrechten 'nogal ruim' interpreteert teneinde afwijkingen van het 'nuttig-effect-beginsel' te beperken.[359]

De doorgifte van persoonsgegevens van een vestiging van een verantwoordelijke binnen de EU naar een daarbuiten valt niet onder de uitzonderingen op het doorgifteverbod. Dit wordt gezien als knelpunt dat kan worden verholpen door dergelijke doorgiften niet te kwalificeren als doorgiften in de zin van artikel 76 Wbp. Ook als knelpunt wordt gezien de onduidelijkheid over de uitzonderingen op dit doorgifte verbod. Sommige auteurs pleiten voor een ruime interpretatie van deze uitzonderingen. De Artikel 29 Werkgroep pleit echter juist voor een restrictieve interpretatie.

4.8 Uitvoeringskosten

De uitvoeringskosten van de privacywetgeving was bij de totstandkoming van de wet[360] een is nog steeds een van de belangrijkste of in elk geval meest besproken 'issues' van de wet.[361] In de parlementaire geschiedenis van de wet is dit dan ook uitdrukkelijk aangemerkt als een van de punten die in de evaluatie van

[355] De Vries 2006, p. 265-267.
[356] Implementatierapport, p. 18-19.
[357] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[358] Art. 29 Werkgroep 2005b, p. 9-10.
[359] Als voorbeelden noemt de werkgroep: EHRM 17 januari 1970, 2689/65 (Delcourt) en EHRM 6 september 1978, 5029/71 (Klass) < www.echr.coe.int/echr>.
[360] Vgl. *Kamerstukken II* 1997-1998, 25 892, nr. 5, p. 9, 14-15; *Kamerstukken II* 1998-1999, 25 892, nr. 6, p. 12, 24-25; *Kamerstukken II* 1998-1999, 25 892, nr. 8, p. 4-6, 9, 24-26; *Handelingen* II 17 november 1999, p. 23-1692-96; Handelingen *I* 1 jui 2002, p. 34-1624-1625. 34-1633-34.
[361] Vgl. Projectgroep Wet Bescherming Persoonsgegevens, *Lasten van de Wbp: Rapportage aan de Commissie Administratieve Lasten,* Den Haag, 19 april 1999.

de wet moet worden meegenomen.[362] Over de omvang van deze uitvoeringskosten van de wet en de richtlijn is veel onderzoek gedaan, zowel voorafgaand aan de inwerkingtreding van de wet als daarna. [363] Uit het Implementatierapport blijkt dat in veel gevallen de wijzigingsvoorstellen vooral gericht waren op het verminderen van de uitvoeringskosten van de wetgeving, alsmede dat de Commissie terughoudend is wat dit betreft omdat deze voorstellen zouden kunnen leiden tot een lager beschermingsniveau:

> 'Where amendments have been proposed by stakeholders, the aim is often the reduction of compliance burdens for data controllers. While this is a legitimate end in itself and indeed one that the Commission espouses, the Commission believes that many of the proposals would also involve a reduction in the level of protection provided for. The Commission believes that any changes that might in due course be considered should aim to maintain the same level of protection.'

Over de uitvoeringskosten en de noodzaak deze terug te brengen is het nodige gezegd door de ondernemings- en werkgeversorganisaties.[364] In aanvulling daarop heeft ook het Cbp[365] aangegeven dat hij het belang van lastenverlichting onderschrijft, met name om het draagvlak van de wet te verbeteren:

> 'Niet alleen is het voor het bedrijfsleven belangrijk dat de verlichting van de administratieve lasten voortvarend ter hand wordt genomen, ook is het voor het draagvlak van de Wbp in de samenleving noodzakelijk dat ondernemers zich niet geconfronteerd zien met onnodige lasten als gevolg van de Wbp.'

Uit de inventarisatie die het Cbp daartoe heeft gedaan blijkt dat de toezichthouder tien knel- cq verbeterpunten ziet die achtereenvolgens zien op de meldplicht, het voorafgaand onderzoek, de informatieplichten en kennisnemingsrecht en de doorgifteregels. Het Cbp staat daarbij een wijziging van de wet het Vrijstellingsbesluit voor en ziet weinig in het aanpassen van de privacy-richtlijn. Dit omdat:

> '[w]ijziging van de richtlijn [..] een langdurig proces [is] met een onzekere uitkomst. Het Cbp is van mening dat meer winst te behalen is door pragmatische oplossingen uit te werken. Met het bovenstaande is getracht daaraan een uitwerking te geven. Het wijzigen van het Vrijstellingsbesluit Wbp is op korte termijn te realiseren waardoor nog in 2005 een aanzienlijk besparing haalbaar is. Ook verwacht het Cbp dat aanpassing van de Wbp op redelijk korte termijn tot de mogelijkheden behoort.'

Ook stelt de Commissie dat de privacywetgeving waarmee de richtlijn wordt geïmplementeerd zou moeten leiden tot een vereenvoudigde regelgevende omgeving in de EU. De geharmoniseerde wetgeving wordt geacht:

> 'to simplify the regulatory environment in the interests of both good governance and competitiveness'.[366]

In hetzelfde rapport stelt de Commissie evenwel vast dat de verschillende wijzen waarop lidstaten de richtlijn hebben geïmplementeerd in de weg staan aan zo een vereenvoudigde regelgevende omgeving. De

---

[362] *Handelingen II* 18 november 1999, 24-1813; zie verder resp. *II* 1998-1999, 25892, nr. 6, p. 25; *I* 1998-1999, 25892, nr. 92; *Handelingen II* 18 november 1999, 24-1795.

[363] Zie voor een overzicht van de studie voorafgaand aan de inwerkingtreding van de wet: *Kamerstukken II* 1997–1998, 25 892, nr. 3, p. 32 na de inwerkingtreding kunnen worden genoemd: *Projectgroep Wet Bescherming Persoonsgegevens, Lasten van de Wbp. Rapportage aan de Commissie Administratieve Lasten*, Den Haag 19 april 1999, en de aldaar genoemde studies; ten slotte kan worden genoemd de meer algemene studie naar administratieve lasten van wetgeving: WODC 2003.

[364] Vgl. Projectgroep Wet Bescherming Persoonsgegevens, *Lasten van de Wbp: Rapportage aan de Commissie Administratieve Lasten,* Den Haag, 19 april 1999, m.n. bijlagen; Cbp, Jaarverslag 2004, p. 44.

[365] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.

[366] Implementatierapport, p. 10-11.

Commissie wijst daarbij meer in het bijzonder op de wijze waarop de meldplicht en de doorgifte-regels zijn ingevuld. Deze bevindingen van de Commissie worden deels bevestigd door Cuijpers.[367] die in opdracht van het Adviescollege toetsing administratieve lasten (ACTAL) een onderzoek heeft gedaan naar de verschillen tussen de Wbp en de richtlijn en de invloed daarvan op de administratieve lasten- en regeldruk. In het rapport daarover signaleert zij een aantal mogelijke knelpunten die administratieve lasten tot gevolg zouden kunnen hebben. En daarbij gaat het dan om de lasten die verband zouden kunnen houden met de wijze waarop de richtlijn is geïmplementeerd in de Wbp. De conclusie van het rapport is dat:

> '[v]rijwel alle onderwerpen die in de literatuur naar voren zijn gebracht als bronnen van administratieve lasten [..], gezien de bewoordingen van de richtlijn en de Wbp, aangepast [kunnen] worden in een poging de administratieve lasten voortvloeiend uit de Wbp te verminderen.'

Uit het onderzoek blijkt evenwel niet waar in de praktijk de problemen ervaren worden met (buitensporige) administratieve lasten. Wel wordt in het rapport aangegeven dat administratieve lastenverlichting vooral gewenst is waar het gaat om de meldplicht en het vrijstellingensysteem, de informatieplichten en het vergunningsysteem voor doorgiften van persoonsgegevens naar derde landen. Dit is in lijn met het Implementatierapport van de Commissie en de meeste literatuur hierover.[368] Overkleeft-Verburg merkt in een noot bij een uitspraak van de Afdeling bestuursrechtspraak op dat de Europese Commissie in het kader van een dereguleringsslag ook de administratieve verplichtingen uit de richtlijn in heroverweging lijkt te nemen.[369]

Als knelpunten worden gezien de uitvoeringkosten van vooral de meldplicht en het vrijstellingensysteem, de informatieplichten en het vergunningsysteem voor doorgiften van persoonsgegevens naar derde landen.

Meldplicht

Over de ingewikkeldheid van de meldplicht merkt de Commissie in haar Implementatierapport op dat deze in een aantal lidstaten – welke dat zijn wordt niet aangegeven – moet worden vereenvoudigd. Daarbij wordt evenwel aangetekend dat de richtlijn voorziet in de mogelijkheden voor de nationale wetgevers om vergaande uitzonderingen op de meldplicht te formuleren:

> 'Many submissions argue for the need to simplify and approximate the requirements in Member States as regards the notification of processing operations by data controllers. The Commission shares this view, but recalls that the Directive already offers the Member States the possibility to provide for wide exemptions from notification in cases where low risk is involved or when the controller has appointed a data protection official. These exemptions allow for sufficient flexibility while not affecting the level of protection guaranteed. Regrettably, some Member States have not availed themselves of these possibilities. However, the Commission agrees that, in addition to wider use of the existent exemptions, some further simplification would be useful and should be possible without amending the existing Articles'. [370]

De Commissie geeft niet aan welke lidstaten meer gebruik zouden moeten maken van de mogelijkheden om meer verwerkingen uit te zonderen van de meldplicht. In een wat oudere publicatie stelt De Heij,[371]

---

[367] Cuijpers 2006.
[368] Vgl. ACT II 2004. p. 14.
[369] ABvRS 21 september 2005, AU2998, *JB* 2005, 307, m.nt. G. Overkleeft-Verburg.
[370] Implementatierapport, p. 12 en 17-18.
[371] De Heij 2001, p. 59-63.

senior beleidsmedewerker bij het Cbp, dat het Vrijstellingsbesluit vanwege het hoge abstractieniveau aanleiding zal geven tot interpretatievragen. Maar als een erg groot probleem ziet deze auteur dit niet.

> '[deze interpretatievragen zijn] onvermijdelijk, maar met gebruikmaking van een dosis gezond verstand zullen deze problemen kunnen worden opgelost.'

Uit het rapport van ACTA II[372] blijkt dat het Nederlandse meldingssysteem volgens het Cbp in vergelijking met die van andere lidstaten eenvoudig is. Toch ziet de toezichthourder[373] hier nog ruimte voor verbetering. Zo merkt Cbp-voorzitter Kohnstamm[374] op dat Nederland wat de meldingen betreft in Europa voorop loopt met het Vrijstellingsbesluit. Echter, om ervoor te zorgen dat men niet meldt als dat niet hoeft nodig is, stelt hij voor het besluit te redigeren. Daarmee kunnen de administratieve lasten, ook bij het Cbp zelf, volgens hem behoorlijk worden verminderd. Verder sluit hij niet uit dat het aantal vrijgestelde verwerkingen in het Vrijstellingsbesluit wordt uitgebreid.

In dat verband stelt Blok[375] de door de wetgever gekozen systematiek ter discussie. De wetgever heeft beoogt dat 'het leeuwendeel' van de verwerkingen wordt vrijgesteld van de meldplicht. En dan ligt volgens deze auteur voor de hand om uit te gaan van een beperkte meldingsplicht, en niet van een ruime plicht waarop weer uitzonderingen worden geformuleerd. De auteur stelt voor om de meldplicht bijvoorbeeld te beperken tot die gevallen waarin de gegevensverwerking buiten de betrokkene om plaatsvindt. Dergelijke geluiden zijn, niet toevallig, ook veel te horen van de kant van ondernemers- en werkgeversorganisaties.[376] Meer daarover in hoofdstuk 5 van dit rapport.

De meldplicht wordt, gelet op de daaraan verbonden uitvoeringskosten, algemeen gezien als een knelpunt. Over de oplossingen verschillen de meningen. Het Cbp en vooralsnog ook de Commissie staan een uitbreiding van het aantal vrijgestelde verwerkingen voor. Ook wordt voorgesteld om uit te gaan van een beperkte genormeerde meldplicht in plaats van genormeerde vrijstellingen.

Doorgifteregels

In het voorgaande is, bij de bespreking van de doorgifteregels, al vastgesteld dat met name de vergunning voor een doorgiftevergunning wel wordt aangeduid als 'een ergerniswekkende administratieve last'. Verder bleek al dat ook het Cbp[377] de vergunning niet nodig vind als er gebruik wordt gemaakt van de modelovereenkomsten. Om deze reden heeft de toezichthouder de minister het verzoek gedaan om hiervoor een vrijstelling te creëren. Verder dringt het Cbp aan op het verduidelijken van de in dat kader gebruikte begrippen – dat laatste ziet hij niet als iets wat hij zelf kan doen maar wat moet gebeuren door de Artikel 29 Werkgroep. Daarnaast wijst het Cbp op de mogelijkheden om via Binding Corporate Rules, – een regeling voor alle internationale gegevensdoorgiftes binnen een concern – te komen tot een vermindering van de uitvoeringskosten.

In aanvulling daarop kan nog worden gewezen op de oplossingen die de Commissie aandraagt in het Implementatierapport voor de administratieve lasten die het gevolg zijn van de verplichting om een vergunning te verkrijgen voor de doorgifte of om deze te melden. De Commissie ziet daar voor zichzelf ook een belangrijke rol weggelegd, namelijk door het beoordelen van de passende beschermingsniveau dat in derde landen of via modelovereenkomsten wordt geboden:

> 'Transfers requiring authorisation and notification do of course create a considerable administrative burden, both for data exporters and for supervisory authorities. It is there-

372 ACT II 2004, p. 14.
373 Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
374 Holvast 2005c, p. 114-119.
375 Blok 2002, p. 318.
376 NVO-NCW, brief d.d. 15 december 2004, kenm. 04/15.098/Gf/CV.227.
377 Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.

> fore desirable that more use be made of the "block authorisations" provided for in Articles 25(6) and 26(4) of the Directive. These have so far produced only four adequacy findings for third countries (Hungary, Switzerland, Canada, and the US Safe Harbor) and two sets of standard contractual clauses, one for transfers to data controllers in third countries and one for transfers to processors. More work is needed on the simplification of the conditions for international transfers.

De uitvoeringskosten in verband met de doorgifteregels worden algemeen gezien als een belangrijk knelpunt. Om deze kosten te beperken wordt voorgesteld om de relevante begrippen en uitzonderingen te verduidelijken, alsmede om de vergunningplicht af te schaffen als gebruik wordt gemaakt van de modelovereenkomsten. Verder kan de Commissie een bijdrage leveren aan de oplossing van dit probleem door het beschermingsniveau van derde landen en modelovereenkomsten te beoordelen.

Informatieplicht

De informatieplicht wordt door Holvast geduid als een 'een molensteen van administratieve lasten'. [378] Naar aanleiding daarvan stelt Kohnstamm[379] dat transparantie een basisvoorwaarde is voor vertrouwen tussen leverancier en consument en overheid en burger. Om deze reden moet transparantie en de daarvoor te maken kosten volgens hem niet worden gezien als last, maar als:

> 'een investering die primair behoort bij de primaire investeringen die een bedrijf of overheid hoort te verrichten. En dan is het geen last meer.'

Toch heeft het Cbp in zijn brief aan de Minister van Justitie wel aangegeven hoe in zijn visie de uitvoeringskosten die verband houden met de informatieplichten kunnen worden teruggebracht, namelijk door de open normen van deze verplichtingen te concretiseren. En daarbij ziet het Cbp ook voor zichzelf een mogelijke rol. Hij merkt op dat de informatieplichten van artikel 33 en 34 Wbp:

> 'veel open normen [bevatten] hetgeen onzekerheid over wat vereist is teweegbrengt. Deze onzekerheid veroorzaakt onnodige nalevingkosten. Het Cbp heeft in 2005 de informatieplicht als een hoofdthema. Er zal gewerkt worden aan een standaardisering van de informatieplicht. Dit kan ofwel betekenen dat de huidige open normen nader worden ingevuld, ofwel dat aanpassing van de Wbp vereist is. Verduidelijking op dit terrein zal leiden tot lastenverlichting bij de verantwoordelijken.'

Meer concreet is de aanbeveling van het Cbp om de informatieplicht met betrekking tot het verzetsrecht voor direct marketing verwerkingen af te schaffen. Als de betrokkenen reeds op de gebruikelijke wijze zijn geïnformeerd hoeft dat volgens de toezichthouder niet nogmaals te gebeuren via dag-, nieuws-, of huis-aan-huisbladen of op een andere geschikte wijze, zoals artikel 41, derde lid, Wbp verlangt.

De uitvoeringskosten die verband houden met de informatieplichten worden gezien deels gezien als iets waarin verantwoordelijken moeten investeren, maar deels ook als een probleem dat kan worden opgelost door open normen in te laten vullen door het Cbp.

Rechten van betrokkenen

Waar het gaat om de kennisnemingrechten van betrokkenen meent het Cbp[380] dat de kosten die verband houden met de uitvoering daarvan alleen kunnen worden teruggebracht door een redelijke uitwerking en uitleg van de desbetreffende bepaling. De toezichthouder geeft aan dat:

---

[378] Holvast 2005c, p. 114-119.
[379] Holvast 2005c, p. 114-119.
[380] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.

> 'het inzagerecht ingevolge artikel 35 Wbp [kan] niet gewijzigd (…) worden zonder het huidige beschermingsniveau aan te tasten. Het schrappen van de verplichting van de verantwoordelijke om dit schriftelijk te doen leidt tot een verlaging van het beschermingsniveau van de betrokkenen. Vermindering van de administratieve lasten die worden veroorzaakt door het inzagerecht is naar het oordeel van Cbp vooral mogelijk door een redelijke uitwerking en uitleg van de bepalingen.'

Hoe dat moet worden bereikt en welke rol het Cbp voor zichzelf ziet, is niet helemaal duidelijk. Van belang is dat er inmiddels wel enige rechtspraak over het kennisnemingrecht van artikel 35 Wbp is. Maar daarmee zijn volgens verschillende auteurs[381] de onzekerheden over de reikwijdte en inhoud van dit recht nog niet opgehelderd. Overkleeft-Verburg wijst in dit verband ook op onduidelijkheid rond de uitleg van het kostenbesluit, waarin de vergoeding rond de afwikkeling van een kennisnemingverzoek van een betrokkene wordt geregeld. Anders dan de Afdeling bestuursrechtspraak stelt zij zich op het standpunt dat de maximale vergoeding van €22,50 voor iedere afzonderlijke gegevensverwerking geldt en niet als maximum vergoeding voor één kennisnemingverzoek, dat meerdere gegevensverwerkingen kan beslaan, moet worden gelezen.[382]

Ook de uitvoeringskosten die verband houden met het kennisnemingsrecht worden gezien als knelpunt. Het Cbp meent dat deze alleen kunnen worden opgelost door een redelijke uitwerking en uitleg van de bepalingen.

4.9 Technologie-onafhankelijkheid

Hoewel de Wbp uitdrukkelijk beoogt technologie-onafhankelijk te zijn is er juist met betrekking tot dit aspect nogal wat kritiek. In het voorgaande is al gewezen op de kritiek van Terstegge,[383] die vraagtekens plaatst bij de technologie-onafhankelijkheid van de begrippen in de Wbp en opmerkt dat deze onder druk komen te staan door de invoering van RFID-toepassingen en innovatieve concepten als 'ubiqituous computing' of 'ambient intelligence'. Volgens Terstegge betekenen dergelijke technologische ontwikkelingen het einde van de privacywetgeving zoals wij die nu kennen.

Prins[384] gaat niet zover. Wel stelt zij dat er meer zou moeten worden gekeken naar de effecten van de nieuwe technologieën die Terstegge noemt in plaats van naar gegevens:

> 'the question is not so much whether personal data are processed; they always are and will be, whether for legitimate or for unlawful purposes. [...]. The problem is rather how personal data are processed, in what context, and towards what end.'

En:

> 'the discussion on adequate mechanisms for the protection of personal data must be a discussion on whether, and to what extent, the statistical models, profiles and algorithms that are used to generate knowledge about our individual behaviour, social and economic position as well as personal interests belong in the public domain.'

Blok[385] vindt dat de Wbp niet goed aansluit bij 'de wereld van internet'. Evenals Zwenne,[386] Hustinx[387] en Terstegge[388] baseert hij dit mede op de uitkomsten van het Lindqvist-arrest.[389] Blok wijst in dat verband

---

[381] Van den Bergen 2005, p. 296-306; Berkvens 2005a, p. 119-121; Holvast 2005a, p. 323-327; Rank & Haasjes 2005; van Schoonhoven 2006a, p. 200-205; Zwenne & Webbink 2006, p. 2-8.
[382] ABRvS 8 maart 2006, *LJN* AV3894, zaaknr. 200505195/1, *JB* 2006, 119, m.nt. G. Overkleeft-Verburg.
[383] Terstegge 2005, p. 39-40.
[384] Prins 2004b; Prins 2004a, p. 34-47.
[385] P.H. Blok 2005b, p. 247.

ook op de specifieke wetgeving die in aanvulling op de Wbp nodig is om spam en cookies te regelen. Veel eerder, namelijk toen het ontwerp van de richtlijn in de Tweede Kamer werd besproken, werd overigens ook al naar voren gebracht dat de richtlijn tekortschiet

> 'omdat nieuwe technologische ontwikkelingen, zoals bij internet, er niet in zijn opgenomen.'[390]

Ondanks het streven naar technologie-onafhankelijkheid wordt als algemeen knelpunt gezien dat de wet niet aansluit bij technologische ontwikkelingen en meer in het bijzonder de wereld van internet

4.10 Conclusies

In deze paragraaf worden de in dit hoofdstuk geïdentificeerde knelpunten geplaatst in het perspectief van de drie invalshoeken, zoals die zijn uiteengezet in hoofdstuk 1.

Formeel-juridisch

De onduidelijkheden met betrekking tot de invulling of concretisering van de vele open normen in de wet wordt algemeen gezien als groot en belangrijk knelpunt. De veronderstelling van de wetgever dat deze onduidelijkheden zouden kunnen worden opgehelderd in de rechtspraak blijkt maar in beperkte mate juist te zijn. Onduidelijkheden doen zich onder ander voor waar het gaat om de interpretatie van de verschillende toestemmingsvarianten in de wet, met name in een online-omgeving. Ondanks het streven naar technologie-onafhankelijkheid wordt als algemeen knelpunt gezien dat de wet niet aansluit bij technologische ontwikkelingen en meer in het bijzonder de wereld van internet. Ook de gevoeligheid van sommige gegevens, met name de bijzondere gegevens, is niet altijd duidelijk, omdat deze gevoeligheid contextafhankelijk is.

Aan het systeem van verschillende bestuurs- en civielrechtelijke procedures zijn volgens enkele auteurs nadelen verbonden, zoals forumshopping en in rechterlijke competenties en afbreuk van rechtseenheid.

Waar het gaat om internationale doorgifte wordt vooral het vergunningvereiste dat ook geldt als gebruik wordt gemaakt van de modelcontracten ervaren als een knelpunt. Ook als knelpunt wordt gezien de onduidelijkheid over de uitzonderingen op dit doorgifteverbod. De voorgestelde oplossingen lopen uiteen van een flexibelere en ruimere interpretatie van deze begrippen tot juist een restrictievere interpretatie.

Waar het gaat om transparantie worden ook knelpunten gesignaleerd die in verband worden gebracht met de interpretatie van de relevante begrippen. Handhaving en zelfregulering worden gezien als middelen om deze knelpunten te verhelpen. Ook de te ruime werking van de meldplicht wordt algemeen gezien als een knelpunt.

Handhaving en naleving

Veel auteurs zien de op verschillende gebieden vastgestelde onduidelijkheden en onbepaaldheid van de wettelijke begrippen als een knelpunt dat de naleving van de wet belemmert en in de weg kan staan aan technologische ontwikkeling en innovatie. Voorgestelde oplossingsrichtingen lopen uiteen van een terughoudende interpretatie en een verstandige flexibele toepassing tot een vergaande heroverweging van de wijze van regulering. Volgens sommige auteurs leidt het algemene, omnibuskarakter van de wet tot grote

---

386 Zwenne 2004, p. 66-69; zie ook het verslag van een ELSA-congres over 'Privacy en de weg naar de informatiesamenleving' van M. Dijkstra, B. Poort en A van Zeevaart 2006, p. 75.
387 Hustinx 2005, p. 62-65.
388 Terstegge 2005, p. 39-40.
389 EHvJ 6 november 2003, (Bodil Lindqvist) C101/01.
390 *Kamerstukken II* 1994-1995, 23 900 VI, nr. 13, p. 1.

knelpunten, waarvan de ingewikkeldheid en de inflexibiliteit het meest in het oog springen. Een enkele andere auteur meent dat een omnibus noodzakelijk is om alle betrokken belangen in hun onderlinge samenhang te kunnen bezien. En uit de in het kader van dit onderzoek gehouden expertmeeting bleek dat er onder de aanwezigen vrijwel geen behoefte was aan sectorale wetgeving in plaats van de Wbp.

Een knelpunt voor verantwoordelijken met vestigingen in meerdere lidstaten is dat verschillende nationale privacywetten van toepassing zijn op de verwerkingen van deze vestigingen, zodat er binnen één en hetzelfde concern meerdere regimes gelden. Ook dat maakt naleving van de wet lastig. Van dezelfde orde zijn knelpunten die verband houden met de omstandigheid dat de Wbp enerzijds van toepassing kan zijn op verwerkingen die weinig verband houden met Nederland, terwijl anderzijds de wet niet van toepassing kan zijn op verwerkingen die wel specifiek verband houden met Nederland. Een enkele auteur ziet de extraterritoriale toepassing van de wet, gelet op de bescherming van betrokkenen, niet als probleem maar als een voordeel.

De gedeeltelijke niet-toepassing van de wet op verwerkingen met journalistieke, artistieke en literaire doeleinden leidt ook tot vragen over de handhaving van de bepalingen die wel van toepassing zijn, maar lijkt geen aanleiding te geven tot reële knelpunten. Een ruimere interpretatie van de journalistieke, artistieke en literaire doeleinden wordt gesuggereerd om websites meer buiten de werking van de wet te brengen. Er worden verder knelpunten gesignaleerd waar het gaat om het vaststellen van wie hebben te gelden als verantwoordelijken en op wie de materiële normen van de wet dus primair van toepassing zijn.

De (te) ruime werking van de meldplicht en de onduidelijkheden met betrekking tot de informatieplichten worden, gelet op de daaraan verbonden uitvoeringskosten, algemeen gezien als een knelpunt dat aan de naleving van de wet in de weg staat. Over de oplossingen verschillen de meningen. Waar het gaat om de meldplicht staan het het Cbp en vooralsnog ook de Commissie een uitbreiding van het aantal vrijgestelde verwerkingen voor. Anderen stellen voor uit te gaan van een beperkte genormeerde meldplicht in plaats van genormeerde vrijstellingen. De uitvoeringskosten die verband houden met de informatieplichten worden gezien deels gezien als iets waarin verantwoordelijken maar moeten investeren, maar deels ook als een probleem dat kan worden opgelost door open normen in te vullen. Ook de uitvoeringskosten die verband houden met het kennisnemingsrecht worden gezien als knelpunt. Het Cbp meent dat deze alleen kunnen worden opgelost door een redelijke uitwerking en uitleg van de bepalingen.

De uitvoeringskosten in verband met de doorgifteregels worden algemeen gezien als een belangrijk knelpunt. Om deze kosten te beperken wordt voorgesteld om de relevante begrippen en uitzonderingen te verduidelijken, alsmede om de vergunningplicht af te schaffen als gebruik wordt gemaakt van de modelovereenkomsten. Verder kan de Commissie een bijdrage leveren aan de oplossing van dit probleem door het beschermingsniveau van derde landen en modelovereenkomsten te beoordelen.

Beeldvorming en bekendheid

Waar het gaat om de beeldvorming en bekendheid van de wet komt uit verschillende onderzoeken een gevarieerd, soms zelfs tegenstrijdig beeld naar voren, met name waar het gaat om transparantie van verwerkingen en de naleving van de wet. In onderzoek worden knelpunten gesignaleerd met betrekking tot kennis bij verantwoordelijken over de wettelijke informatieplichten: veel verantwoordelijken menen dat zij niet zijn gehouden om betrokkenen te informeren over de doeleinden waarvoor zij persoonsgegevens verwerken. En toch blijkt uit ander onderzoek weer dat verantwoordelijken over het algemeen wel goed bekend zijn met de wettelijke kennisnemings- en verbeteringsrechten, en dat de meerderheid van hen geen moeite heeft om daaraan te voldoen aan. Ook blijkt dat betrokkenen veel belang hechten aan de transparantie van de hen betreffende verwerkingen, maar tegelijkertijd het gevoel hebben maar weinig daarin inzicht te hebben.

De niet-naleving van de Wbp wordt in verband wordt gebracht met een gebrek aan bekendheid of bewustwording bij verantwoordelijken. In dat verband kan ook worden gewezen op onderzoek, waaruit

blijkt dat de bekendheid van het Cbp gering is en dat maar weinig betrokkenen aangegeven zich tot de toezichthouder te zullen wenden als zij problemen zouden hebben met de bescherming van persoonsgegevens. Ook blijken zij voor hun gevoel maar weinig zicht te hebben op de op hun betrekking hebbende registraties.

Hoofdstuk 5: Private sector

5.1 Inleiding

Dit hoofdstuk bevat een weergave van de de meest in het oog springende knelpunten in de private sector. Daarbij worden tot de private sector gerekend die organisaties die niet tot de publieke of semi-publieke sector behoren. Dat zijn in ieder geval de rechtspersonen en organisaties die volledig of in aanzienlijke mate worden gefinancierd uit particuliere middelen. De knelpunten worden besproken aan de hand van de in hoofdstuk 1 onderscheiden thema's te weten: werkingssfeer en toepassing, normatieve kaders, zelfregulering, transparantie en rechten van betrokkenen, rechtsbescherming en toezicht en internationale doorgifte. Ook wordt ingegaan op knelpunten die samenhangen met de uitvoeringskosten en de technologie-onafhankelijkheid van de Wbp.

5.2 Werkingssfeer en toepassing

Uit de bestudeerde literatuur blijkt dat de knelpunten ten aanzien van de werkingssfeer en toepassing zich concentreren op de afbakening van begrippen zoals 'persoonsgegevens' en 'verwerken', de toepasselijkheid van de Wbp bij internationale verhoudingen, bij fusies en overnames en bij gegevensstromen binnen een groep van ondernemingen. Ook blijken er knelpunten te zijn bij de toepassing van de Wbp in het geval van internet en spam. Daarnaast worden in literatuur knelpunten gesignaleerd ten aanzien van de aansluiting van de Wbp op andere wetten.

5.2.1 Begrippen

Onduidelijke begrippen

Uit de literatuur blijkt dat de definities van bepaalde begrippen uit de Wbp, zoals 'persoonsgegevens' en 'verwerken', in de private sector tot onduidelijkheden en daarmee tot knelpunten aanleiding geeft. Het persoonsgegevens-begrip is een niet afgebakend begrip waardoor de vraag wat persoonsgegevens zijn, afhankelijk is van de interpretatie die er aan wordt gegeven. In het voorgaande is al gewezen op de inbreng van de RCO.[391] Deze vertegenwoordiger van ondernemersorganisaties meent dat beeld- en geluidmateriaal niet zouden moeten worden aangemerkt als persoonsgegevens voor zover het materiaal niet gebruikt wordt in de context van de persoonlijke levenssfeer.[392] De RCO vindt dat niet alle verwerkingen (bijvoorbeeld het verzamelen, verstrekken, raadplegen) van beeldmateriaal zoals foto's, noodzakelijkerwijs persoonsgegevens bevatten. Voor zover beeldmateriaal toch persoonsgegevens zou bevatten, zou dit veelal triviale zaken betreffen. De toekenning van rechten aan betrokkenen en het naleven van de informatieplicht in zulke zaken, zou een te vergaande mate van invloed van betrokkenen op verantwoordelijken met zich meebrengen.

Ook Cuijpers[393] signaleert in haar proefschrift dat er onduidelijkheden zijn rondom de afbakening van het begrip persoonsgegevens. Zij meent echter dat, om in Europa een werkbaar systeem van gegevensbescherming te hebben, het noodzakelijk is dat de uitleg van de reikwijdte van het begrip persoonsgegeven op Europees en niet op nationaal niveau moet worden bepaald. De doelstelling van de privacy-richtlijn

---

[391] Zie par. 4.2.1 van dit rapport. Dit betreft een officieel ingediende opinie bij de Europese Commissie naar aanleiding van de evaluatie van de Europese privacyrichtlijn.
[392] De RCO meent dat de privacyrichtlijn niet zozeer de bescherming van persoonsgegevens centraal zou moeten stellen, maar de bescherming van privacy; zie RCO 2003.
[393] Cuijpers 2006, p. 12.

omvat haar inziens het scheppen van een vrij en geharmoniseerd gegevensverkeer tussen de lidstaten. Cuijpers doet ook een voorstel om de definitie van persoonsgegevens nader af te bakenen. Zo stelt zij voor om onderscheid te maken tussen persoonsgegevens en professionele gegevens. Ervaringen uit de praktijk leren volgens haar dat de toepasselijkheid van de Wbp op professionele informatie tot onwerkbare situaties kan leiden. Het zou een onnodige last op het bedrijfsleven drukken als zelfs een simpele handeling als het afgeven van een visitekaartje onder de Wbp zou vallen terwijl reeds op grond van de algemene zorgvuldigheidsnormen en informatieplichten, gebruikers van de op het kaartje gedrukte gegevens verplicht zijn om hier op een zorgvuldige en voor de betrokkene voorzienbare wijze mee om te gaan. Cuijpers wijst er wel op dat onder professionele gegevens geen 'human resource data' begrepen moet worden omdat deze gegevens zeer ingrijpend kunnen zijn voor de betrokkene als privé-persoon. Op basis van deze gegevens vindt bijvoorbeeld de beoordeling van de persoon als werknemer plaats. Bij een slechte beoordeling kan ontslag volgen, hetgeen ook voor de werknemer als privé-persoon zeer ingrijpend kan zijn.[394]

Het verwerken van persoonsgegevens omvat elke denkbare soort van handeling die men met persoonsgegevens kan verrichten. Hierover brengt de RCO naar voren dat niet elke handeling die gepaard kan gaan met persoonsgegevens, onder het begrip 'verwerken' zou dienen te vallen omdat dit een te grote toepasselijkheid van de Wbp met zich zou meebrengen. Zo stelt de RCO dat daar waar sprake is van het (technisch) bewaren of doorgeven van gegevens zoals door een tussenpersoon of service provider, de voordelen van de toepasselijkheid van de Wbp op een dergelijke handeling niet duidelijk zijn.[395]

Concernverhoudingen

De onbeperkte toepasselijkheid van de Wbp brengt ook onduidelijkheid en daarmee knelpunten met zich mee bij fusies, overnames en bij gegevensverwerkingen die binnen een concern plaatsvinden. Cuijpers merkt hierover op dat begrippen zoals 'verantwoordelijke', 'bewerker' en 'derde' in de genoemde situatie niet makkelijk toepasbaar zijn, dan wel onwenselijke gevolgen met zich mee kunnen brengen. Zij meent dat hier verandering in moet komen en dat moet worden nagedacht over de noodzakelijkheid om bijvoorbeeld in alle gevallen onderdelen van hetzelfde concern als derden ten opzichte van elkaar te beschouwen.[396] De diverse knelpunten die zich voordoen bij fusies, overnames en in concernverhoudingen, komen ook bij de verschillende andere thema's van dit hoofdstuk verder naar voren.

In het voorgaande is uiteengezet[397] dat uitvoeringsproblemen in concernverhoudingen volgens Terstegge kunnen worden verminderd door het in Nederland introduceren van het in Duitsland bediscussieerde maar niet ingevoerde 'Konzern Privileg'. Dit houdt in dat persoonsgegevens binnen een concern kunnen worden uitgewisseld als ware het een verstrekking binnen één verantwoordelijke concernmaatschappij. Een voorwaarde voor toepassing van dit 'Konzern Privileg' is dat er binnen het concern een uniform beleid wordt gevoerd over hoe om te gaan met de verwerking van persoonsgegevens. Toepassing van dit concept zou onder meer gevolgen hebben voor de definitie van verantwoordelijke, voor het Vrijstellingsbesluit, alsmede voor het vereiste van een bewerkersovereenkomst als de ene groepsvennootschap gegevens verwerkt ten behoeve van de ander.

De onduidelijkheden en onbepaaldheid van de belangrijkste begrippen in de Wbp, zoals persoonsgegevens, verwerking, verantwoordelijke en bewerker, geeft in de private sector aanleiding tot problemen. De weinig beperkte reikwijdte van de wet blijkt met name te leiden tot knelpunten waar het gaat om internationale concernverhoudingen.

---

394 Cuijpers 2003, p. 111-112.
395 RCO 2003.
396 Cuijpers 2003, p. 111.
397 Zie par. 4.2.1 van dit rapport.

5.2.2 Toepassing

De toepasselijkheid van de Wbp bij internationale gegevensstromen en internet levert knelpunten op als geprobeerd wordt een antwoord te vinden op de vraag welk rechtstelsel van een lidstaat van toepassing is op een bepaalde verwerking van persoonsgegevens. Dit blijkt op zijn minst genomen complex. Zo blijkt het in veel gevallen ondoenlijk om een verantwoordelijke aan te wijzen bij typische internetverschijnselen zoals weblogs, webfora en zoekmachines.

Ook bestaat onduidelijkheid of internet service providers of internet access providers moeten worden aangemerkt als 'verantwoordelijke' in de zin van de Wbp. Formeel-juridisch is de Wbp vaak wel van toepassing, maar feitelijk biedt de Wbp nauwelijks toegevoegde waarde in het reguleren van gegevensverwerkingen op internet. Winkelhorst[398] komt in een artikel over privacy en zoekmachines tot de conclusie dat de Wbp wel van toepassing kan zijn, maar niet uitgerust is om de dynamiek van de zoekmachines te kunnen normeren. Lodder e.a.[399] menen dat de Wbp onvoldoende houvast biedt om spam juridisch aan te pakken omdat de handhaving niet adequaat kan worden opgepakt door het feit dat de verzenders van spam zich veelal bevinden in landen waar de Wbp niet van toepassing is en zelfs als dit wel zo zou zijn, er maar beperkte mogelijkheden zijn om tegen de verzending van spam op te treden.

5.2.3 Aansluiting bij andere wetten

Uit literatuur blijkt dat naast een op onderdelen onduidelijk begrippenkader en de toepassingsproblemen van de Wbp, ook knelpunten worden ervaren en beschreven ten aanzien van de aansluiting van de Wbp op specifieke regelgeving in de private sector zoals de Databankenwet en de Wet elektronische handel. Al genoemd zijn[400] Koning & De Vries[401], die aangeven dat de Wbp complicerend kan werken ten aanzien van de Databankenwet doordat belangrijke begrippen uit beide wetten niet op elkaar aansluiten of niet zijn geharmoniseerd. Ook blijkt uit een discussiedocument van het Cbp dat de 'Aanpassingswet inzake richtlijn elektronische handel'[402] en de Wbp geen gelijke begrippen kennen. Zo wordt in het discussiedocument beschreven dat een term als de 'verantwoordelijke' uit de Wbp, geen pendant kent in de Wet elektronische handel. Om toch een gemeenschappelijk kader te kunnen creëren voor een ondernemingsactiviteit die zowel onder de Wbp als de aanpassingswet valt, kiest het Cbp er vooralsnog voor om voor de term 'verantwoordelijke' aansluiting te zoeken bij de bepalingen rondom aansprakelijkheid in de aanpassingswet.[403]

In de literatuur worden knelpunten gesignaleerd ten aanzien van de aansluiting van de Wbp met met name de Databankenwet en de Aanpassingswet inzake richtlijn elektronische handel.

5.3 Normatieve kaders

5.3.1 Wijze van normering

De normatieve kaders van de Wbp houden ten aanzien van gegevensverwerkingen voor een groot deel rekening met de beginselen van proportionaliteit en subsidiariteit. Dat wil zeggen dat voordat tot een verwerking wordt overgegaan, onder meer eerst nauwgezet door de verantwoordelijke moet worden beoordeeld of een verwerking is toegestaan en of die wel noodzakelijk is. Ook zal de verantwoordelijke vooraf

398 Winkelhorst 2005, p. 146-154.
399 Lodder e.a. 2004, p. 73.
400 Zie par. 4.3.1 van dit rapport.
401 Koning & de Vries 2003, p. 58.
402 *Stb.* 2004, 210.
403 Cbp, Publicatie van persoonsgegevens op internet, 17 mei 2006, p. 20.

moeten beoordelen of niet met een minder ingrijpende verwerking kan worden volstaan. Verder dient hij te beoordelen of een eventuele verdere verwerking wel verenigbaar is met het doel waarvoor de gegevens werden verkregen. Om deze belangrijke voorvragen te kunnen beantwoorden, geeft de Wbp een normatief kader dat soms heel specifiek en strikt is, en soms weer heel erg abstract en onbepaald. Uit de literatuur blijkt dat de Wbp niet in alle gevallen een duidelijk beeld geeft van wat mag en wat niet. Er blijken knelpunten in de private sector bestaan ten aanzien van het het toestemmingvereiste en de vage normen vervat in het 'gerechtvaardigd belang' (art. 8, onder f, Wbp) en andere vage normen in de wet.

5.3.2 Verwerkingsgrondslag

Artikel 8 Wbp bevat een limitatieve opsomming van zes verwerkingsgronden. Eén van die gronden is dat de betrokkene voor de verwerking van zijn gegevens zijn ondubbelzinnige toestemming verleend. Cuijpers stelt vast dat over deze verwerkingsgrond binnen de lidstaten verschillend wordt gedacht. Dit betreft zowel de wijze waarop toestemming kan worden gegeven als de wijze waarop toestemming weer kan worden ingetrokken. Daarnaast stelt zij dat de uitleg die de Artikel 29 Werkgroep geeft aan het begrip toestemming in arbeidsrelaties tot knelpunten aanleiding geeft – dit omdat de werkgroep ervan uit gaat dat er alleen sprake kan zijn van toestemming als de werknemer de mogelijkheid heeft om de toestemming zonder nadeel in te trekken.[404] Cuijpers meent dat als uitgangspunt zou moeten gelden dat zolang toestemming op informatie berust en bovendien ondubbelzinnig en vrij gegeven is, er voor de wijze waarop toestemming verleend wordt, geen additionele voorwaarden moeten gelden. Zij stelt dat voor toestemming in arbeidsrelaties het van belang is dat de machtspositie van de werkgever ten opzichte van de werknemer meegewogen wordt bij de beoordeling of de toestemming vrij gegeven is. Toestemming zou haar inziens echter niet op voorhand uitgesloten moeten worden geacht omdat een vrij verkeer van gegevens hierdoor ernstig belemmerd kan worden. Als voorbeeld noemt zij een online cv-databank met cv's en foto's van werknemers. In de visie van de Artikel 29 werkgroep zou toestemming geen verwerkingsgrondslag kunnen vormen, terwijl veel werknemers zichzelf kennelijk wel graag in een cv-databank wil zien worden opgenomen.[405]

Gegevens kunnen niet alleen op de grondslag van toestemming van de betrokkene worden verwerkt. De uitvoering van een wettelijke taak of het gerechtvaardigd belang van een ander kan soms ook een grondslag voor verwerking vormen. Zo stelt het Cbp[406] dat Zorgverzekeraars Nederland, de Nederlandse Vereniging van Ziekenhuizen en de Vereniging van Academische Ziekenhuizen ten behoeve van het halen van regres, graag een melding van zorgverleners ontvangen wanneer één van hun cliënten mogelijk slachtoffer is geworden van een ongeval. Het Cbp meent dat in een dergelijke situatie kan worden uitgegaan van veronderstelde toestemming, hetgeen het verbod op het verstrekken van gegevens die vallen onder het medisch beroepsgeheim doorbreekt.[407]

Een knelpunt bij een andere verwerkingsgrond vormt het volgende. Door Merkus wordt beschreven dat het twijfelachtig is dat er een gerechtvaardigd belang aanwezig kan worden geacht in het geval er sprake is van uitwisseling van persoonsgegevens in het kader van een due diligence onderzoek. Zij meent dat, op basis van uitspraken in het verleden van de rechtsvoorganger van het Cbp, de Registratiekamer, persoonsgegevens nauwelijks zouden mogen worden uitgewisseld. Een dergelijke verstrekkende terughoudendheid

---

[404] Art. 29 Werkgroep 2001, p. 23: 'the article 29 working party takes the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment'.
[405] Cuijpers 2003, p. 112.
[406] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
[407] Zie voor een nadere uitwerking hoofdstuk 7.

werkt volgens Merkus vaak belemmerend bij een overname.[408] Zo is het soms essentieel om van bepaalde werknemers of soorten van werknemers, persoonsgegevens uit te wisselen omdat het interessant kan zijn om die werknemers verbonden te laten blijven aan de over te nemen onderneming.

De Wbp blijkt in de praktijk beperkingen te stellen aan de toegankelijkheid van persoonsgegevens waar dat volgens onder meer het Verbond van Verzekeraars niet nodig zou moeten zijn. Het verbond meent dat zij meer toegang zou moeten kunnen krijgen tot persoonsgegevens dan volgens de huidige opvattingen over de verwerkingsgrondslag van het gerechtvaardigde belang (art. 8, onder f, Wbp) mogelijk lijkt. Als voorbeelden van dergelijke niet of lastig te verkrijgen gegevens worden genoemd: gegevens omtrent een sterfdatum of doodsoorzaak – gegevens waartoe verzekeraars zeggen toegang te behoeven als er sprake is van een levensverzekering heeft met de (overleden) betrokkene.[409]

Verder blijkt uit onderzoek van het Cbp[410] dat er met name waar het gaat om particuliere recherchebureau's en handelsinformatiebureau's, sprake is van veel onduidelijkheden over de informatieplichten, bewaartermijnen, het gebruik van externe informatiebronnen, doelomschrijving van het onderzoek, de vastlegging van de gebruikte onderzoeksmethoden voor onderzoek.

De Wbp geeft niet in alle gevallen een duidelijk beeld van wat kan en wat niet. De verantwoordelijke dient zelfstandig te bepalen hoe het normatieve kader van de Wbp kan worden toegepast op gegevensverwerkingen. Uit literatuur blijkt dat er in ieder geval knelpunten in de private sector bestaan ten aanzien van het begrip 'toestemming' en het 'gerechtvaardigd belang' en de (on)rechtmatige toegang tot (bijzondere) gegevens door derden.

5.4 Zelfregulering

5.4.1 Gedragscodes

Met sectorbrede gedragscodes kunnen de algemene normen van de Wbp voor een bepaalde sector nader worden ingevuld en geconcretiseerd. De binnen een sector gebruikelijke richtlijnen en/of tradities voor de omgang met persoonsgegevens kunnen hiermee ook expliciet worden gemaakt en een sterke verbindende status verkrijgen. Naast het kunnen concretiseren van de normen van de Wbp, is een gevolg van een aangenomen gedragscode dat het Cbp terugtreedt als eerstelijns toezichthouder,[411] met name als met de gedragscode een onafhankelijke geschillenbeslechting in het leven is geroepen.

Toekenning voordelen

In de private sector is een aantal gedragscodes opgesteld die door het Cbp zijn goedgekeurd. Het opstellen en het verkrijgen van de goedkeuring door het Cbp, is een tijdsintensief, langdurig en daarom kostbaar proces. Deze omstandigheden maken dat het opstellen van gedragscodes nog niet een echt hoge vlucht heeft genomen. Op dit moment zijn in totaal zeven gedragscodes van kracht. Cuijpers stelt in haar rapport voor ACTAL tegen deze achtergrond voor om het opstellen van gedragscodes aan te moedigen door hier tegenover voordelen te bieden die thans ontbreken.[412]

---

[408] Merkus 2002, p. 18.
[409] Zie ook *Stcrt.* 26 maart 2004, nr. 60.
[410] Cbp, 'Particuliere recherche en bescherming van persoonsgegevens, 23 mei 2006, p. 3-4; Cbp 2003; Van Ringelestijn 2006.
[411] Van de Pol 2000, p. 1141-1157.
[412] Cuijpers 2006, p. 42.

Betekenis gedragscodes

In enkele verschillende uitspraken lijkt de civiele rechter[413] ervan uit te gaan dat gedragscodes kunnen derogeren aan de wet, hetgeen volgens enkele auteurs leidt tot knelpunten. Ook is er sprake van een knelpunt in het geval van een geschil tussen het Cbp en een deelnemer aan een gedragscode over de uitleg van bepalingen van een door toezichthouder goedgekeurde gedragscode. Zo kan het Cbp dreigen met het intrekken van zijn goedkeurende verklaring en daarmee de status van de gedragscode verminderen. Echter, intrekking van een gedragscode kan in voorkomende gevallen een te zware sanctie zijn. Het stilzwijgend laten bestaan van een op onderdelen onwenselijke en/of onrechtmatige gedragscode leidt tot rechtsonzekerheid.[414]

Zelfreguleringstekort

Nouwt constateert een zelfreguleringstekort waar het gaat om het gebruik van ICT. Deze auteur wijst op de mislukking van het internet-zelfreguleringsinitiatief WebTrader in zowel Nederland als het Verenigd Koninkrijk. Doel van WebTrader, een initiatief van onder andere de Consumentenbond, was het 'vertrouwen van de consument in het winkelen via internet te vergroten'. Als een internetwinkel bij WebTrader was aangesloten betekende dat onder meer dat de winkel ook daadwerkelijk bestond en dat consumenten een besteld product binnen de daarvoor geldende termijn kregen thuisbezorgd. Bovendien was er een 'niet goed geld terug garantie'. WebTrader is per 1 januari 2002 gestopt, in het Verenigd Koninkrijk vooral omdat het niet efficiënt zou zijn. Nouwt vindt dit opmerkelijk omdat zelfregulering juist efficiënter zou moeten zijn dan overheidsregulering.[415]

Het door Nouwt geconstateerde zelfreguleringstekort betreft niet alleen gedragsgerichte, informerende, contractuele en geschilbeslechtende instrumenten. Ook wat betreft de techniekgerichte instrumenten valt zijns inziens een zelfreguleringstekort te signaleren. Uit onderzoek verricht in opdracht van de Europese Commissie kan naar zijn mening worden geconcludeerd dat er behoefte is aan bewustzijnbevordering van privacy bevorderende technieken bij consumenten, bedrijfsleven en overheden. Vaak blijkt men niet hoe deze technieken toe te passen.

Nouwt concludeert verder dat zelfregulering onvoldoende waarborgen biedt voor de bescherming van de privacy van de internetconsument. Met name transparantie, rechtszekerheid en naleving zijn punten van zorg. Nouwt meent dat zelfregulering weliswaar een rol van betekenis zou kunnen spelen, maar dan in combinatie met andere sturingsmechanismen. Hij denkt met betrekking tot internetconsumenten vooral aan aanvulling in de vorm van centrale overheidsregulering en de toepassing van door de consument zelf te treffen technische maatregelen. Nouwt meent dat dit laatste vooralsnog ook tekort schiet waardoor er een belangrijke rol voor centrale overheidsregulering zou overblijven.

Uit literatuur blijkt dat knelpunten bij gedragscodes zich voordoen bij de inzet die gemoeid is met het opstellen van een gedragscode en de plaatsbepaling in het recht bij geschillen omtrent de betekenis van een gedragscode. Als instrument voor zelfregulering ten aanzien van internetconsumenten blijken gedragscodes te kort te schieten.

5.5 Transparantie en rechten van betrokkenen

In veel gevallen beschikken ondernemingen over persoonsgegevens zonder dat de betrokkenen daarvan weten. De Wbp biedt bescherming tegen de (informatie)ongelijkheid die als gevolg hiervan kan optreden

---

[413] Rechtbank Amsterdam 19 mei 2005, *LJN* AT5858 en dezelfde rechtbank nogmaals op 10 november 2005, *LJN* AU6428.
[414] Zie voor een voorbeeld: Cbp, 17 maart 2006, z2005-1028.
[415] Nouwt 2005, p. 123.

in de (machts)verhouding tussen een onderneming en een betrokkene, onder meer door de meldplicht, de verplichting om de betrokkene vooraf te informeren over zijn identiteit en de doeleinden van de verwerking van diens persoonsgegevens, alsmede om 'nadere informatie' te verschaffen voorzover dit nodig is om een 'behoorlijke en zorgvuldige' gegevensverwerking jegens de betrokkene te waarborgen. Uit het literatuuronderzoek blijkt dat er vooral sprake is van knelpunten waar het gaat om deze verplichtingen. Deze worden hieronder toegelicht.

5.5.1 Meldplicht

Invulling van het meldingsformulier wordt door veel ondernemingen niet makkelijk geacht. Tevens zou de elektronische variant van het meldingsformulier, het meldingsprogramma, niet gebruiksvriendelijk zijn. Sommige gegevensverwerkingen zijn vrijgesteld van de melding omdat de wetgever hiervan vond dat dit veel voorkomende verwerkingen betrof met geringe invloed op de persoonlijke levenssfeer van betrokkenen. Een beroep op een vrijstelling is echter niet eenvoudig, doordat het Vrijstellingsbesluit zeer gedetailleerd is. Indien reeds aan één onderdeel van een vrijstellingsbepaling niet wordt voldaan doordat bijvoorbeeld nog een ander persoonsgegeven wordt verwerkt dan limitatief opgesomd in de vrijstelling, dan moet er toch gemeld worden.

Een door Merkus[416] en Van Essen[417] genoemd voorbeeld betreft het due diligence onderzoek dat wordt gedaan bij de voorgenomen overname van de ene onderneming door de andere. Bij zo een onderzoek worden in de zgn. 'dataroom' door partijen die bij een overname betrokken zijn, veel gegevens uitgewisseld, waaronder persoonsgegevens zoals personeels-, salaris-, en debiteuren/crediteurenadministraties. Deze administraties zijn in beginsel vrijgesteld van de meldingsplicht. Echter, het doeleinde dat de betreffende gegevens kunnen worden verwerkt in het kader van een due diligence onderzoek, staat niet vermeld in het Vrijstellingsbesluit. Dit betekent dat de uitwisseling in de dataroom, gemeld moet worden bij het Cbp. Tevens dient de melding voorafgaand aan de uitwisseling plaats te vinden. Een vrijstelling van de meldingsplicht ziet verder ook niet op een verwerking waarbij meer dan één verantwoordelijke is betrokken. Van Essen signaleert hier een knelpunt. Gelet op het vertrouwelijke karakter van een overname, kan naar haar mening niet verlangd worden dat er voorafgaand aan een gegevensuitwisseling wordt gemeld bij het Cbp. Daarnaast zijn er meerdere verantwoordelijken bij een due diligence onderzoek betrokken zoals de advocaten van de wederpartij en/of die wederpartij zelf. Die zullen allemaal voor zichzelf moeten melden. Volgens Van Essen dient het Vrijstellingsbesluit dan ook te worden aangepast om standaardverwerkingen zoals die van personeels-, salaris-, en debiteuren/crediteurenadministraties, niet verplicht te hoeven melden voorafgaand aan de situatie waar in een dataroom in het kader van een due diligence onderzoek, gegevens worden uitgewisseld.

Tijdens de bijeenkomst met domeindeskundigen die in het kader van dit onderzoek werd gehouden, kwam naar voren dat het Vrijstellingsbesluit vaak alleen op hoofdlijnen wordt doorgenomen; het zogenoemde 'koppensnellen'. De vraag die een onderneming zich dan stelt is of bijvoorbeeld een debiteurenadministratie is vrijgesteld van de melding. Zodra men dan in het Vrijstellingsbesluit stuit op het kopje 'debiteurenadministratie' leest men niet verder zodat ook geen kennis wordt genomen van de voorwaarden waaronder een dergelijke administratie vrijgesteld kan zijn van de meldplicht.

Onder andere Cuijpers[418] en het Cbp[419] hebben aangegeven hoe het systeem van meldingen en vrijstellingen kan worden vereenvoudigd. In dat verband heeft het Cbp geschat dat ca. 55.000 verwerkingen uit het bedrijfsleven alsnog kunnen worden vrijgesteld en dat bestaande meldingen (welke ook een onderhouds-

[416] Merkus 2002, p. 17.
[417] Van Essen 2003, p. 361-362.
[418] Cuijpers 2006, p. 44.
[419] Cbp, 7 december 2004, z2004-1086.

plicht met zich meebrengen) alsnog in aanmerking zouden komen voor een vrijstelling. Het Cbp heeft er daarom bij de Minister van Justitie voor gepleit dat het Vrijstellingsbesluit beter toegankelijk wordt gemaakt en wordt uitgebreid.

Bedrijven met vestigingen in meerdere lidstaten van de Europese Unie lopen tegen een specifiek knelpunt aan, namelijk dat de meldplicht zeer uiteenlopend in de lidstaten is geïmplementeerd. De Artikel 29 Werkgroep heeft dit knelpunt onderkend en onderzoekt dan ook sinds 2004 of voor deze bedrijven één standaard meldingsformulier kan worden ontwikkeld. Vooralsnog is een dergelijk standaard meldingsformulier echter nog niet beschikbaar.[420]

De RCO [421] staat een andere oplossing voor. Deze ondernemersorganisatie stelt voor dat de verplichting om te melden alleen zou moeten gelden indien er sprake is van een gegevensverwerking waarvoor een voorafgaand onderzoek als bedoeld in artikel 31 Wbp vereist is, omdat juist die verwerkingen een gevaar voor de persoonlijke levenssfeer met zich mee kunnen brengen en gebaat zijn bij meer transparantie. Voor alle overige verwerkingen meent de RCO dat de meldplicht een grote administratieve last omvat voor zowel de verantwoordelijke als de toezichthouder, zonder dat een relevante toegevoegde waarde aan de melding te ontdekken zou zijn.[422]

5.5.2 Informatieplichten voor verantwoordelijken

Een verantwoordelijke dient voorafgaand aan de gegevensverwerking de betrokkenen te informeren over tenminste zijn identiteit en het doel van de verwerking. De privacy-richtlijn op grond waarvan de informatieplicht in de Wbp is opgenomen, bepaalt echter alleen dat betrokkenen geïnformeerd moeten worden over de verwerking van hun persoonsgegevens, en niet dat deze informatieplicht vóór het moment van verkrijging van de informatie geldt. Het voorafgaand informeren levert een extra (financiële) last op voor verantwoordelijken. Een voorbeeld waar dit als knelpunt naar voren kwam betreft het gebruik van gegevens van auto-eigenaren uit het Kentekenregister door belangenbehartigers van de automobielbranche. Het Cbp[423] oordeelde dat het gebruik van deze gegevens voor het versturen van reclame alleen mag als betrokkenen daarover van tevoren geïnformeerd zijn en de mogelijkheid hebben gehad daartegen bezwaar te maken. Een ander, reeds genoemd voorbeeld betreft het voorafgaand informeren in het geval van een due diligence onderzoek bij een bedrijfsovername. Merkus[424] merkt op dat het vertrouwelijke karakter in de weg kan staan aan het voorafgaand informeren. Ook het feit dat er meerdere verantwoordelijken betrokken zijn, vormt een extra complicerende factor.

Behalve zijn identiteit en de doeleinden van de verwerking van de gegevens, dient de verantwoordelijke ook ingevolge artikel 33, derde lid Wbp en 34, derde lid, Wbp 'nadere informatie' te verstrekken voor zover dat gelet op de 'aard van de gegevens', de 'omstandigheden waaronder zij worden verkregen' of het 'gebruik dat ervan wordt gemaakt', nodig is om tegenover de betrokkene een 'behoorlijke en zorgvuldige verwerking te waarborgen'. Deze beide bepalingen bevatten zodoende vijf(!) open normen hetgeen bij de verantwoordelijke rechtsonzekerheid teweegbrengt over wat vereist is.

De rechtsonzekerheid omtrent de inhoud en omvang van de informatieplicht veroorzaakt ten slotte ook onnodige uitvoeringskosten. Het Cbp[425] heeft dit probleem eveneens onderkend aangegeven te werken aan standaardisering van de informatieplicht. Dit heeft evenwel nog niet geleid tot concrete resultaten..

---

[420] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[421] RCO 2003.
[422] Zie ook par. 4.5 en 4.8 van dit rapport.
[423] Cbp Uitspraak 8 september 2004, z2004-0724.
[424] Merkus 2002, p. 18.
[425] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.

Uit de literatuur komt het beeld naar voren dat er in de private sector knelpunten zijn bij het melden van een gegevensverwerking en het zich (niet) kunnen beroepen op het Vrijstellingsbesluit. Verder laat literatuur zien dat er knelpunten zijn bij het vormgeven en naleven van de informatieplicht.

5.5.3 Rechten van betrokkenen

Uit de literatuur blijkt dat er sprake is van een aantal knelpunten is ten aanzien van het kennisnemingsrecht specifiek in de financiële sector, het 'Besluit kostenvergoeding rechten betrokkene Wbp', het correctierecht en de publicatieplicht bij verwerkingen voor direct marketing.

Kennisnemingsrecht

Ondanks dat de rechten die aan een betrokkene toekomen veel invloed kunnen hebben op een verantwoordelijke, kwam tijdens de bijeenkomst met domeindeskundigen naar voren dat niet veel organisaties sinds de inwerkingtreding van de Wbp, praktische ervaring hebben opgedaan met de uitoefening door betrokkenen van hun rechten. Dit beeld is anders in de financiële sector. Zo is, en wordt er nog steeds, geprocedeerd over de uitoefening van het kennisnemingsrecht door bankcliënten van Dexia. In rechtspraak en literatuur[426] over de Dexia-zaak gesignaleerde knelpunten, betreffen de nog niet eenduidig beantwoorde vragen of een recht op kopie bestaat, of inzage moet worden gegeven in persoonlijke werknotities van werknemers van de verantwoordelijke, of bulk aan- en verkoopbewijzen van effecten persoonsgegevens zijn, of opgestelde risicoprofielen persoonsgegevens zijn, of analoog opgenomen telefoongesprekken zijn aan te merken als een bestand in de zin van de Wbp, in welke situaties misbruik van het recht op inzage kan worden gemaakt en wanneer de uitzonderingsgrond van artikel 43, onder e, Wbp toepassing vindt. Ook zijn er vragen of het belang bij inzage door de betrokkene moet worden aangetoond. [427]

Reconstructieplicht

Het gerechtshof Arnhem vernietigde op 11 juli 2006[428] een uitspraak van de rechtbank Zutphen, waarin van een financiële instelling werd verlangd dat een bepaalde gegevensverwerking zou worden gereconstrueerd. Volgens het hof rust op een bank niet de verplichting rust om alle persoonsgegevens die op enig moment in haar elektronische systemen kunnen rondgaan, vast te leggen. Omdat dit de transparantie van gegevensverwerkingen zou kunnen beperken kan dit worden gezien als knelpunt voor betrokkenen.Aan de andere kant zou het aannemen van een reconstructieplicht de desbetreffende financiële instellingen in voorkomende gevallen voor grote problemen stellen.

Kostenvergoeding

In het voorgaande[429] is al kort ingegaan op het Besluit kostenvergoeding Wbp en de kosten die in rekening mogen worden gebracht voor een afschrift van een röntgenfoto. Uitgangspunt is dat een verantwoordelijke maximaal €0,23 per pagina mag vragen aan een betrokkenen voor een inzageverzoek tot een maximum van €4,50 per inzageverzoek. Dit is alleen anders als het overzicht meer dan 100 pagina's beslaat in welk geval de verantwoordelijke maximaal € 22,50 per inzageverzoek mag vragen. In veel gevallen zijn deze bedragen te laag om de kosten te dekken die moeten worden gemaakt als het gaat om het verstrekken van afschriften van een röntgenfoto.

Waar het gaat om transcripties van opgenomen telefoongesprekken (die bijvoorbeeld zijn vastgelegd ten behoeve van de telefonische verkoop van producten en diensten) is er sprake van onduidelijkheid over de

[426] Van Schoonhoven 2006b; Zwenne & Webbink 2006; Rank & Haasjes 2005; Van den Bergen 2005.
[427] Zie ook par. 4.5 van dit rapport.
[428] Gerechtshof Arnhem 11 juli 2006, zaaknr. 120/2006 (niet gepubliceerd).
[429] Zie par. 4.5 van dit rapport.

omvang van het kennisnemingsrecht. Het genereren van een transcriptie vergt een aanzienlijke inspanning van de verantwoordelijke. Op grond van de tekst van voornoemd kostenbesluit kan hiervoor niet meer dan €4,50 worden verlangd van de betrokkene die gebruik maakt van zijn kennisnemingsrecht. Ook een knelpunt is dat onduidelijk is welk bedrag in totaal voor een inzageverzoek in rekening kan worden gebracht dat mede ziet op opgenomen telefoongesprekken. Het genoemde besluit spreekt over maximumbedragen per inzageverzoek. Bij een strikte interpretatie van het besluit, valt daar echter ook de situatie onder waarin vele, soms wel tientallen, telefoongesprekken beschikbaar zijn. In gevallen waarin de transcripties meer dan 100 pagina's beslaan, kan een verantwoordelijke tot maximaal €22,50 vragen voor het gehele inzageverzoek. Van Schoonhoven[430] suggereert dit op te lossen door het ter beschikking stellen van elektronische kopieën of samenvattingen van bestanden.

Aanvulling of correctie

Naast inzage in de door een verantwoordelijke vastgelegde gegevens kan een betrokkene ook verwijdering of aanvulling vragen van zijn gegevens, afhankelijk van de situatie. Zo stelt Heuver[431] ten aanzien van het onderwerp 'credit scoring', dat aanvulling van de gegevens meer waarde heeft dan verwijdering, aangezien door de aanvulling informatie in het bestand van een handelsinformatiebureau kan worden genuanceerd. Heuver meent dat het echter moeilijk is om aan te geven of een dergelijke aanvulling altijd een concreet effect heeft op de creditscore. Verder is van belang dat er nog veel onduidelijkheid bestaat over de uitleg van artikel 42 Wbp dat bepaalt dat niemand onderworpen kan worden aan een beslissing die wordt genomen op basis van een geautomatiseerde gegevensverwerking. Heuver stelt dat indien een betrokkene meent dat gegevens onjuist zijn, die persoon moeite moet doen om dit aan te tonen. In feite bepaalt echter het handelsinformatiebureau zelf of er voldoende grond is om op een dergelijk verzoek van een betrokkene in te gaan. Heuver acht dit onwenselijk.

Publicatieplicht direct marketing

Een betrokkene heeft ook het recht zich te verzetten tegen een verwerking van zijn gegevens voor direct marketing. Artikel 41 derde lid Wbp bepaalt dat de verantwoordelijke die voornemens is persoonsgegevens aan derden te verstrekken of voor rekening van derden te gebruiken, minstens eenmaal per jaar betrokkenen bekend maakt met het recht van verzet middels publicatie via een of meer dag-, nieuws-, of huis-aan-huis-bladen of op een andere geschikte wijze. Met deze publicatieplicht beoogde de wetgever dat de burger meer weet heeft van gegevensverwerkingen en zodoende zelf in staat is te bepalen of zijn gegevens door een verantwoordelijke aan derden mochten worden verstrekt. In de praktijk blijkt dat aan deze publicatieplicht nauwelijks gehoor werd gegeven. Tevens was er de kritiek dat een betrokkene sowieso bij elke direct mailing geïnformeerd moest worden over de verwerking van zijn gegevens, waarmee een publicatie overbodig zou zijn. Het Cbp[432] heeft daarom de Minister van Justitie per brief in overweging gegeven om deze informatieverplichting nader te bekijken. Het Cbp heeft de minister voorgesteld nader te bezien of deze verplichting vervangen kan worden voor een eenvoudiger en effectievere maatregel, dan wel kan worden afgeschaft.

Er is een aantal knelpunten ten aanzien van de inhoud en reikwijdte van het kennisnemingsrecht, de invulling van het correctierecht, en de werking van de publicatieplicht bij verwerkingen voor direct marketing. Ook de (beperkte) omvang van kostenvergoeding leidt tot knelpunten.

[430] Van Schoonhoven 2006b, p. 203-204.
[431] Heuver 2003, p. 55-61.
[432] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.

5.6 Toezicht en rechtsbescherming

Tegen bepaalde beslissingen van de verantwoordelijke kan een betrokkene zich tot de rechtbank wenden met het verzoek de verantwoordelijke te veroordelen alsnog aan het verzoek van de betrokkene te voldoen. In literatuur wordt een aantal knelpunten gesignaleerd die met deze civiele rechtsgang te maken hebben. Het schort daarbij met name aan bekendheid met de Wbp bij rechters en de niet eenduidigheid en hoogdrempeligheid van de civiele procedure.

Het toezicht op en de handhaving van de Wbp door het Cbp, raakt sterk aan de uitoefening van de beleidsvrijheid die aan het Cbp is toebedeeld. Ook ten aanzien daarvan blijken er knelpunten te zijn.

5.6.1 Toezicht

Focus toezicht en publicatiebeleid

Het Cbp kan op verschillende wijzen toezicht uitoefenen. Zo kan het op verzoek klachtonderzoek (art. 60 Wbp) doen, voorlichting geven (art. 51 Wbp), bemiddelen in geschillen (art. 47 Wbp), ambtshalve onderzoek (art. 60 Wbp) verrichten of een voorafgaand onderzoek instellen (art. 31 Wbp). Onderdeel van de uitoefening van het toezicht is ook de organisatorische uitvoering van de toezichtstaak en de scheiding tussen de wettelijke taak van het Cbp en de Minister van Justitie. De functionaris voor de gegevensbescherming fungeert als interne toezichthouder van een verantwoordelijke. Ook de functionaris komt dientengevolge bepaalde bevoegdheden toe.

Uit een TNS NIPO onderzoek naar de perceptie van burgers over de Wbp komt naar voren dat burgers vinden dat de aandacht van het Cbp zich beter op bedrijven zou kunnen richten dan op de overheid. Een vraagpunt dat in het onderzoeksrapport naar voren kwam is of het Cbp door middel van communicatie en voorlichting moet bijdragen aan een maatschappelijk klimaat waarin het vertrouwen in de manier waarop organisaties omgaan met persoonsgegevens groeit, of dat dit een eigen verantwoordelijkheid voor de organisaties is. En als het Cbp daarover zou gaan communiceren, wat daar dan tegenover zou moeten staan van de kant van deze organisaties.[433] In het voorgaande is uiteengezet[434] dat het Cbp als uitgangspunt hanteert dat de namen van bedrijven in uitspraken van het Cbp niet worden vermeld, mede met het oog op een zorgvuldige gegevensverwerking en het voorkomen van een verstoring van de markt.

Een voorbeeld hiervan vormen de procedures tussen het Cbp en de Nederlandse Vereniging van Handelsinformatiebureaus (NVH). Het Cbp had in een onderzoek geconstateerd dat een handelsinformatiebureau onrechtmatig gegevens verwerkte. De NVH wenste hierop de naam van het bureau te vernemen zodat het kon bepalen of tegen dat bureau stappen konden worden genomen. Het Cbp weigerde de naam van het bureau te geven en werd uiteindelijk ook door de Afdeling bestuursrecht in het gelijk gesteld.[435] Uit een berichtje op de voorpagina van de Staatscourant[436] kan niettemin worden opgemaakt dat Kohnstamm, voorzitter van het Cbp, ervoor pleit dat het Cbp verplicht zou worden om de naam te noemen van de organisatie die het onderzoekt. Dit omdat het Cbp anders aansprakelijk gesteld kan worden als een bedrijf schade oploopt omdat zijn goede naam is aangetast door een onderzoeksrapport van het Cbp.

Het Cbp lijkt geneigd te zijn om meer gebruik te willen maken van een actief publicatiebeleid in het kader van zijn toezichthoudende taken. In dat verband wordt gedacht aan een wettelijk verplicht verdergaand publicatiebeleid. Vanuit vooral het bedrijfsleven is daar kritiek op.

---

[433] Schildmeijer, Samsons & Koot 2005, p. 23.
[434] Zie par. 4.6.1 van dit rapport.
[435] ABRvS 7 april 2004, *LJN* AO7115.
[436] *Stcrt.* 12 juli 2006.

5.6.2 Rechtsbescherming

Onbekendheid Wbp bij civiele rechters

De FNV stelt in 2002 dat de Wbp betrekkelijk weinig betekenis heeft in civielrechtelijke procedures, en dat maar in beperkte mate gevolgen verbonden zijn aan een schending van deze wet bij het verzamelen van bewijsmateriaal.[437] Verder zouden kantonrechters zeer uiteenlopende oordelen geven op basis van nagenoeg gelijke zaken waarmee de FNV constateert dat de rechtsontwikkeling daarmee niet in de pas loopt met de ons omringende buurlanden, alsmede dat vaak de werkgever in bescherming wordt genomen indien sprake is van een onrechtmatige verwerking van persoonsgegevens.[438] De Hert komt tot een soortgelijke conclusie. Hij meent dat de logica achter de Wbp niet steeds doorgedrongen is in alle rechtsdomeinen.[439] Andere auteurs[440] geven aan dat een schending van de Wbp door de werkgever alleen een rol lijkt te spelen bij het bepalen van de uiteindelijk vast te stellen ontslagvergoeding voor de werknemer.

Geen eenduidige en laagdrempelige rechtsgang

Een ander knelpunt betreft de door de wetgever beoogde laagdrempeligheid[441] en eenduidigheid van de rechtsgang op grond van artikel 45 en 46 Wbp. Van Schoonhoven[442] stelt vast dat rechtbanken bijvoorbeeld van mening verschillen of er wel of geen griffierecht verschuldigd is voor inzageprocedures op grond van de Wbp en of er bij deze procedures wel of geen kostenveroordeling mogelijk is. Daarnaast blijkt voor de executie van een beschikking door een betrokkene, juridische bijstand noodzakelijk. Van Schoonhoven constateert verder dat, omdat het Cbp niet bevoegd is tot het starten van 'proefprocedures' in principiële zaken, afbreuk wordt gedaan aan de laagdrempeligheid van de rechtsgang van de Wbp. Ook geeft hij aan dat de rechtsontwikkeling op principiële punten volledig overgelaten wordt aan de belanghebbende zelf. Van Schoonhoven geeft dan ook in overweging dat de wet op deze punten wordt aangepast.

Termijn indiening verzoekschrift

De termijn waarbinnen een verzoekschrift op grond van artikel 45 en 46 Wbp bij de rechtbank kan worden ingediend, is zes weken na het nemen van een afwijzende beslissing door een verantwoordelijke op een verzoek van een belanghebbende. Dit moment en daarmee het begin van deze termijn is echter niet in alle situaties even helder. Zo bepaalt artikel 41 tweede lid Wbp dat de verantwoordelijke 'terstond' gehoor dient te geven aan een ingesteld verzet tegen verwerking met het oog op werving voor commerciële of charitatieve doelen. Een verzoek tot beëindiging van de verwerking van gegevens van een betrokkene in geval van direct marketing, dient de eerstvolgende keer dat tot verwerking van gegevens wordt overgegaan te zijn geëffectueerd. In beginsel kan dan niet tot verwerking van gegevens worden overgegaan zolang niet alle verzoeken tot beëindiging zijn verwerkt. Er is echter geen verplichting voor de verantwoordelijke om de betrokkene ervan op de hoogte te stellen dat de honorering is gebeurd. Het Cbp constateert hierover dat het daardoor in de praktijk onduidelijk is wanneer de termijn aanvangt waarbinnen de betrokkene een verzoekschrift kan indienen bij de rechtbank of het Cbp als de verantwoordelijke zijn verzoek niet inwilligt. Het Cbp heeft de Minister van Justitie verzocht een oplossing te vinden voor dit probleem waarbij

---

[437] Vgl. Hoge Raad 21 april 2001, *NJ* 2001, 421 (Wennekes lederwaren).
[438] FNV 2003, p. 2.
[439] De Hert 2002, p. 26-30.
[440] Jager 2003, Even 2003, Bijlsma & Homan 2003 en Lacevic & Zondag 2004. Zie verder ook paragraaf 4.6.2.
[441] Vgl. art. 46, vierde lid, Wbp.
[442] Van Schoonhoven 2006a, p. 62; Van Schoonhoven 2006b, p. 90.

een evenwicht gezocht wordt in de administratieve lasten van het bedrijfsleven en de rechtszekerheid voor de burger.[443]

Tegen bepaalde beslissingen van de verantwoordelijke kan een belanghebbende zich tot de rechtbank wenden met het verzoek de verantwoordelijke te veroordelen alsnog aan het verzoek van de belanghebbende te voldoen. Het schort daarbij met name aan bekendheid bij rechters met de Wbp, waardoor er geen eenduidige rechtsgang is en afbreuk wordt gedaan aan de beoogde laagdrempeligheid van de civiele procedure.

5.7 Internationale gegevensdoorgifte

Persoonsgegevens mogen alleen naar een land buiten de Europese Unie worden doorgegeven voor verwerking, indien dat land een passend beschermingsniveau waarborgt. Welke landen een passend beschermingsniveau hebben, beoordeelt de Europese Commissie. Voor een beperkt aantal landen heeft de Europese Commissie in de afgelopen jaren vastgesteld dat van een passend beschermingsniveau sprake is. Veel doorgiften vinden echter plaats naar landen zonder passend beschermingsniveau. Doorgiften naar een dergelijk land is alleen mogelijk als er sprake is van een uitzonderingsgrond op het verbod tot doorgifte of wanneer een vergunning door de Minister van Justitie is afgegeven. Voor doorgiften naar de Verenigde Staten is er een alternatief beschikbaar dat deels op basis van zelfregulering tot stand is gekomen, en de zgn. 'Safe Harbor regeling'. Indien een onderneming voldoet aan de eisen die worden gesteld om een 'Safe Harbor' te worden, kan doorgifte naar die onderneming plaatsvinden, ook al bevindt die onderneming zich in een land zonder passend beschermingsniveau.[444] Met betrekking tot een en ander blijkt er sprake van knelpunten, met name waar het gaat om de interpretatie van de uitzonderingsgronden, zelfregulering, het doorgiftevergunningvereiste, en de rechtsbescherming bij de vergunningprocedures.

5.7.1 Werking

Internet

In verband met de Lindqvist-procedure stelt Berkvens[445] vast dat het de vraag is of dan het raadplegen van de informatie via internet wel een doorgifte vormt. Het Hof heeft hier echter geen uitspraak over gedaan. Winkelhorst & Ter Linden-Smith[446] lijken te vinden dat de internetgebruiker moeite moet doen om informatie op internet te traceren zoals het intikken van een internetadres. Zolang informatie niet geautomatiseerd wordt doorgezonden, is er volgens hen geen sprake van een doorgifte. Zwenne[447] constateert verder ten aanzien van de doorgifteproblematiek dat de door het Hof gegeven uitleg van de privacy-richtlijn een technologiespecifieke uitzondering formuleert en dat daarmee de privacy-richtlijn veel minder technologieneutraal blijkt te zijn dan wel werd aangenomen. Zwenne sluit niet uit dat er in de toekomst nog meer afstand zal worden genomen van het uitgangspunt dat de regelgeving zoveel mogelijk technologieonafhankelijk moet zijn en dat dientengevolge de privacyregelgeving niet eenvoudiger wordt.[448]

Het Lindqvist-arrest laat verder zien dat een nationale wetgever strengere eisen mocht stellen ter bescherming van de privacy en van persoonsgegevens dan die welke uit de privacy-richtlijn volgen. Dit kan ook gevolgen hebben op andere rechtsgebieden. Zo trekken de Wetenschappelijke Raad voor het Regeringsbe-

[443] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[444] Blok 2002, p. 268-271.
[445] Berkvens 2004a, p. 17-20.
[446] Winkelhorst & Van der Linden-Smith 2004, p. 627-631.
[447] Zwenne 2004, p. 425.
[448] Zwenne 2004, p. 66-69; zie ook Blok 2004, p. 30- 36; Kranenborg 2004, p. 415-425.

leid en Alberdingk Thijm[449] uit het arrest van het Hof de conclusie dat de 'vergaande' bescherming zoals die in het arrest naar voren komt, een blokkade zal opwerpen tegen pogingen van bijvoorbeeld de muziekindustrie om inbreukmakers op de intellectuele eigendomsrechten van auteurs op te sporen.

Bescherming door Wbp na doorgifte

Er moet een vergunning worden aangevraagd als een doorgifte naar een derde land zonder passend beschermingsniveau plaatsvindt en ook geen beroep kon worden gedaan op een uitzonderingsgrond. Zowel Thijssen[450] als Cuijpers[451] wijzen erop dat de Wbp, ook zonder de aanwezigheid van een vergunning of uitzonderingsgrond, van toepassing kan zijn, aangezien artikel 4, eerste lid, Wbp bepaalt dat de Wbp van toepassing is op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland. De wet is derhalve van toepassing op verwerkingen buiten de Europese Unie zolang dat gebeurt in de context van activiteiten van een vestiging van de verantwoordelijke. Op basis daarvan meent Thijssen[452] dat artikel 76 en 77 Wbp onnodige eisen stellen aan een doorgifte, omdat de Wbp in die situatie reeds voorziet in een passend beschermingsniveau. Om deze ongereimdheid te adresseren doet Thijssen het voorstel dat het begrip 'doorgifte' niet langer wordt gereserveerd voor doorgiften waarbij de Wbp nog voor een passend beschermingsniveau zorgt. Verder zouden artikel 76 en 77 Wbp gewijzigd kunnen worden. Daarnaast zou artikel 4 eerste lid Wbp aangepast kunnen worden zodat niet langer persoonsgegevens na doorgifte beschermd (kunnen) worden door de Wbp.

Een ander, wellicht nog tijdelijk, knelpunt betreft de doorgifte van passagiersgegevens door vliegtuigmaatschappijen aan inlichtingen en veiligheidsdiensten in de VS. Op 30 mei 2006 heeft het Europees Hof van Justitie[453] bepaald dat de besluiten van de Commissie en de Raad daarover en de Raad niet op de juiste rechtsgrondslag waren gebaseerd en derhalve vernietigd. De Artikel 29 Werkgroep[454] heeft naar aanleiding van de uitspraak van het Hof een opinie aangenomen waarin zij onder meer aangeeft dat:

> '[f]or the middle-long term the Working Party considers it necessary to develop a more coherent approach towards the exchange of passenger data to ensure on a global level both air traffic security and the respect of human rights.'

Volgens de werkgroep is er dus, ondanks de inmiddels gerealiseerde tijdelijke oplossing, nog steeds sprake van een knelpunt.

Het Europese Hof van Justitie heeft in het Lindqvist-arrest voor de eerste maal uitleg gegeven aan de term 'doorgifte'. Deze uitleg zorgt voor discussie in literatuur. Artikel 4 Wbp kan er toe leiden dat persoonsgegevens ook na doorgifte uit Nederland naar een derde land, beschermd worden door de Wbp. In een dergelijke situatie zou geen vergunning voor doorgifte noodzakelijk zijn.

5.7.2 Toepassing en uitzonderingen doorgifteverbod

Uitzonderingsgronden

In artikel 77 eerste lid Wbp staat een aantal uitzonderingsgronden geformuleerd op het verbod tot doorgifte van gegevens. Deze gronden betreffen gedeeltelijk open normen die strikt moeten worden geïnterpreteerd.[455] Voorts bevatten de meeste uitzonderingsgronden een noodzakelijkheidstoets. Dit betekent dat

[449] Alberdingk Thijm 2003, p. 76.
[450] Thijssen 2005, p. 110-113.
[451] Cuijpers 2003, p. 115-119.
[452] Thijssen 2005, p. 110-113; Cuijpers 2003, p. 119.
[453] EHvJ 30 mei 2006, zaken C-317/04 en C-318/04.
[454] Art. 29 Werkgroep 2006b.
[455] Zie onder meer: Art. 29 Werkgroep 2005b, p. 9.

een beroep op een uitzonderingsgrond alleen kan slagen, als rekening is gehouden met de beginselen van proportionaliteit en subsidiariteit. Of dit echter zo is, is een afweging die een verantwoordelijke zelfstandig moet zien te maken. Ten aanzien van de interpretatie van de uitzonderingsgronden komt in literatuur naar voren dat zowel de Artikel 29 werkgroep als het Cbp uit praktijkervaring is gebleken, dat er onduidelijkheid bestaat over de toepassing van de uitzonderingsgronden op het verbod op doorgifte indien er geen sprake is van een adequaat niveau van bescherming, zoals geformuleerd in artikel 26 eerste lid van de privacy-richtlijn, en in Nederlands recht omgezet in artikel 77 eerste lid Wbp. Indien een verantwoordelijke zich kan beroepen op een van deze gronden voor doorgifte, mogen persoonsgegevens worden doorgeven aan een derde land dat geen passend niveau van bescherming heeft zonder dat nadere passende waarborgen moeten worden getroffen.

Het Cbp meent dat onduidelijkheid over de toepassing van de uitzonderingen veelal tot een administratieve last leidt. Zo kan onduidelijkheid er toe leiden dat omwille van het verkrijgen van rechtszekerheid, een vergunning wordt aangevraagd terwijl dit eigenlijk niet hoeft. Jakimowicz & Borrat i Frigola[456] lijken dit standpunt van het Cbp te onderschrijven en stellen vast dat er vaak zekerheidshalve een vergunning wordt aangevraagd om te voorkomen dat de restrictieve uitleg van de uitzonderingsgronden door het Cbp, voor problemen zou kunnen zorgen als geen vergunning was aangevraagd. Om deze problemen op te lossen heeft de Artikel 29 werkgroep[457] een document opgesteld waarin nadere regels worden gegeven voor het toepassen van de uitzonderingsgronden. De werkgroep brengt onder meer naar voren dat het gebruik van een modelcontract of Binding Corporate Rules voorrang dient te hebben op de toepassing van een uitzonderingsgrond. Voorts stelt de werkgroep dat de uitzonderingsgronden restrictief moeten worden geïnterpreteerd.

Naast de knelpunten bij de interpretatie van de bestaande uitzonderingsgronden, lijkt uit literatuur te kunnen worden afgeleid dat de signalering van verschillende andere knelpunten, min of meer beogen de bestaande uitzonderingsgronden uit te breiden. Zo wordt wel opgemerkt dat er geen equivalent van het gerechtvaardigd belang als verwerkingsgrondslag (art. 8, onder f, Wbp) is opgenomen in de uitzonderingsgronden die het doorgifteverbod doorbreken (art. 77, eerste lid, Wbp). Volgens Cuijpers[458] zijn er situaties denkbaar waarin het gerechtvaardigd belang aanwezig is zoals bij routinematige verwerkingen die geen of nauwelijks risico's opleveren voor de persoonlijke levenssfeer van betrokkenen. Cuijpers meent dat een dergelijke grondslag een uitzondering kan vormen op het verbod tot doorgifte zonder dat dus een vergunning behoeft te worden aangevraagd.

Verder blijkt dat het verwerken van personeelsgegevens of 'human resource data' binnen een concern met vestigingen in en buiten de EU, problematisch kan zijn omdat hiervoor een vergunning moet worden aangevraagd. In het voorgaande[459] is aangegeven dat als oplossing wel wordt voorgesteld gebruik te maken van het in Duitsland veel bediscussieerde, maar niet ingevoerde concept van zgn. 'Konzern Privileg'. Dat wil zeggen dat persoonsgegevens binnen één concern worden verwerkt als ware het binnen één en dezelfde verantwoordelijke.[460] Zo is de Artikel 29 werkgroep[461] van mening dat het 'zeer twijfelachtig' is of het begrip 'arbeidsovereenkomst' zo breed kan worden uitgelegd dat doorgifte noodzakelijk is voor de uitvoering van de arbeidsovereenkomst. Omdat een vergunningaanvraag een langdurig traject kan betekenen wordt centralisatie van de genoemde data, hetgeen veelvuldig voorkomt in concerns, bemoeilijkt. Cuij-

---

[456] Jakimowicz & Borrat i Frigola 2006, p. 31-32.
[457] Art. 29 Werkgroep 2005b, p. 10-11.
[458] Cuijpers 2003, p. 115-116.
[459] Zie par. 4.2.1 van dit rapport.
[460] Dit bleek niet zozeer uit de literatuur maar uit interviews die voorafgaand aan het onderhavige onderzoek zijn gehouden.
[461] Art. 29 Werkgroep 2005b, p. 14-15.

pers[462] meent dat het bestaan van een uitzonderingsgrond voor deze categorie van doorgifte, dit knelpunt zou kunnen verhelpen.

Daarnaast blijk dat op grond van de tekst van de Wbp, een vergunning moet worden aangevraagd voor de doorgifte van persoonsgegevens in het kader van een due diligence onderzoek. Als knelpunt merkt Merkus[463] op dat de Registratiekamer reeds oordeelde dat een dergelijke doorgifte het belang van de commerciële partijen dient en niet het belang van de betrokkene. Merkus verbindt daaraan de conclusie dat dit ondernemingen bij de uitvoering van een due diligence onderzoek in een moeilijke positie brengt, waardoor het risico bestaat dat ondernemingen zich niet aan de wet zullen houden. Dit wordt naar haar mening versterkt doordat de Wbp slechts geringe sancties hiertegen bevat.

Safe Harbor

Over de zgn. safe harbor regels, op grond waarvan gegevens kunnen worden doorgegeven naar de VS, merkt Nouwt[464] op dat is gebleken dat deze op zgn. elektronische markten geen succes zijn. Zo zou het bij op deze markt ontbreken aan transparantie, rechtszekerheid en naleving. Nouwt meent verder dat dit zelfreguleringstekort ook lijkt te kunnen worden afgeleid uit het feit dat de Verenigde Staten, het land bij uitstek ten aanzien van zelfregulering, op dit terrein lijken 'om te gaan'. Zo stelt de Federal Trade Commission zich op het standpunt dat zelfreguleringsinitiatieven vanuit het bedrijfsleven op zichzelf niet tot voldoende privacybescherming op de elektronische markt kunnen leiden. Aanbieders van goederen en diensten op internet blijken zich namelijk niet te houden aan de door hen zelf vastgestelde beleidsregels (privacystatements) voor de omgang met persoonsgegevens van consumenten. Hoewel de Federal Trade Commission zelfregulering wel van belang acht, is men inmiddels van mening dat het Amerikaanse congres in aanvulling daarop wetgevingsinitiatieven dient te nemen..

Modelcontracten

Voor het aanvragen van een vergunning kan gebruik worden gemaakt van een drietal modelcontracten. Twee daarvan zijn door de Europese Commissie ontwikkeld en één door het bedrijfsleven zelf. De Europese Commissie heeft bepaald dat bepaalde modelcontracten voor doorgifte naar derde landen voldoende waarborgen bieden voor de bescherming van de persoonlijke levenssfeer. In veel lidstaten is daarom besloten dat het niet nodig is een vergunning aan te vragen als gebruik wordt gemaakt van deze door de Europese Commissie goedgekeurde modelcontracten.

De Wbp bevat geen bepalingen die verantwoordelijken vrijstellen van het aanvragen van een vergunning in het geval dat zij gebruik maken van een door de Europese Commissie goedgekeurd modelcontract. Verantwoordelijken die gevestigd zijn in Nederland moeten dus ook bij gebruikmaking van de modelcontracten een vergunning aanvragen. Veel verantwoordelijken ervaren dit als een ergerniswekkende administratieve last, zo bleek onder meer al in 2003 tijdens een door het Cbp georganiseerde expertmeeting over internationaal gegevensverkeer.[465] Waarschijnlijk dat deze ergernis er ook voor zorgt dat er tot en met 2005 niet meer dan 73 vergunningaanvragen waren ingediend.[466] Jakimowicz & Borrat i Frigola stellen dat veel doorgiften dus onrechtmatig zullen plaatsvinden.

Het voorgaande in acht nemende, acht het Cbp het wenselijk dat het aanvragen van een vergunning achterwege kan blijven als er gebruik wordt gemaakt van ongewijzigde modelcontracten. Het gebruik hiervan brengt met zich mee dat de risico's met betrekking tot de gegevensbescherming na doorgifte gering zijn. Een toetsing voorafgaand aan de doorgifte zou naar de mening van het Cbp onvoldoende toevoegen aan

---

[462] Cuijpers 2003, p. 115-117.
[463] Merkus 2002, p. 16-18.
[464] Nouwt 2005a, p. 123-125.
[465] Cbp, 1 juli 2003, verslag.
[466] Jakimowicz & Borrat i Frigola 2006, p. 31-31.

de gegevensbescherming om deze te rechtvaardigen. Het Cbp heeft de Minister van Justitie laten weten dat de vergunningplicht zou moeten worden afgeschaft als gebruik wordt gemaakt van de ongewijzigde modelcontracten.[467] VNO-NCW, ACTAL en Cuijpers[468] delen het standpunt van het Cbp. Fontein[469] voegt nog een andere overweging aan dit standpunt toe door te suggereren dat het ook mogelijk is dat de Minister van Justitie een categorale vergunning verstrekt in de genoemde gevallen. Een wetswijziging is dan niet nodig.

In sommige gevallen kan niet worden volstaan met de ongewijzigde modelcontracten. Zo zijn de modelcontracten niet toegespitst op gegevensverwerkingen die binnen een concern kunnen plaatsvinden. Om deze reden wordt door de Artikel 29 Werkgroep gewerkt aan een mogelijkheid tot doorgifte van gegevens op grond van zgn. Binding Corporate Rules. Dit zijn interne gedragscodes van multinationale bedrijven over persoonsgegevensverwerking op grond waarvan doorgiften binnen het concern kunnen plaatsvinden. Deze vorm van zelfregulering kan voldoende waarborgen bieden ten aanzien van gegevensbescherming. Het maakt het afsluiten van individuele contracten met zusterorganisaties in derde landen overbodig. Tevens kan op grond van de Binding Corporate Rules een vergunning worden verleend voor alle huidige en toekomstige doorgiften binnen een concern. Het Cbp heeft de Minister van Justitie verzocht deze ontwikkeling te ondersteunen en daar waar mogelijk zowel nationaal als internationaal te stimuleren. Vooralsnog heeft het gebruik van Binding Corporate Rules vanwege tijd die ermee is gemoeid en de kosten die er aan verbonden zijn, geen hoge vlucht genomen.

Rechtsbescherming

Zoals uit het voorgaande blijkt vormt de regelgeving rondom doorgifte een gevoelig onderwerp binnen het bedrijfsleven. Veel aspecten van de regelgeving en het uitvoeringsbeleid van het Cbp worden door bedrijven als overbodig en/of onnodig ervaren. De RCO[470] stelt dat er weinig rechtsbescherming bestaat tegen een negatief oordeel van een toezichthouder in het kader van een vergunningaanvraag.

Veel doorgiften vinden plaats naar landen zonder passend beschermingsniveau. Doorgiften zijn alleen mogelijk als er sprake is van een passend beschermingsniveau, een uitzonderingsgrond op het verbod tot doorgifte of wanneer een vergunning door de Minister van Justitie is afgegeven. Zo zijn er knelpunten rondom de interpretatie van de uitzonderingsgronden, zelfregulering, het aanvragen van een vergunning, ook indien bijvoorbeeld gebruik wordt gemaakt van een modelcontract van de Europese Commissie, en de rechtsbescherming bij de vergunningprocedures.

5.8 Uitvoeringskosten

In het voorgaande[471] is uitgebreid stilgestaan bij de uitvoeringskosten van de Wbp. Veel van de daar genoemde oorzaken kennen een sectoroverstijgend karakter. Voor de private sector is met name een brief van de ACTAL[472] relevant. Daaruit blijkt dat de ACTAL van mening is dat de administratieve lasten voor het bedrijfsleven in de nulmeting te laag zijn ingeschat. De nulmeting per 31 december 2002 is door het Ministerie van Justitie uitgevoerd om een schatting te kunnen geven van de administratieve lasten van de Wbp. De lasten voor het bedrijfsleven werden toen op € 30 miljoen per jaar berekend. Volgens ACTAL zou dit bedrag € 42 miljoen per jaar moeten zijn. De ACTAL geeft als verklaring voor deze hoger berekende lasten dat de oorspronkelijke inschatting van de lasten als gevolg van de Wbp te laag zijn geweest

[467] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086.
[468] ACTAL 2006; Cuijpers 2003, p. 120; VNO-NCW 2004.
[469] Fontein 2004, p. 211.
[470] RCO 2003.
[471] Zie par. 4.8 van dit rapport.
[472] ACTAL 2006.

omdat de Wbp pas op 1 september 2002 in werking was getreden. Verder zouden nog steeds externe privacyspecialisten nodig zijn. De ACTAL stelt:

> 'Nu er meer ervaring is opgedaan met de Wbp blijkt de tijd die bedrijven besteden aan informatieverplichtingen en de frequentie daarvan hoger te zijn dan ingeschat. Ook blijkt inhuur van externe privacyspecialisten door het bedrijfsleven vooralsnog nodig, bijvoorbeeld bij het kennisnemen van de Wbp en het Vrijstellingsbesluit en het verstrekken van informatie aan betrokkenen bij inzage van gegevens.'

Het Cbp[473] en VNO-NCW[474] hebben beide reductievoorstellen gedaan tot een bedrag van minimaal € 4 miljoen lastenverlichting per jaar voor het bedrijfsleven. Het Cbp stelt in zijn brieven dat de reductievoorstellen geen afbreuk doen aan het huidige beschermingsniveau. ACTAL adviseert deze voorstellen zo spoedig mogelijk door te voeren. Verder adviseert ACTAL het kabinet om de vergunningsplicht bij doorgifte van persoonsgegevens naar derde landen af te schaffen en het minst belastende alternatief in te voeren.

Het Cbp heeft naast een toezichthoudende taak ook andere taken. Zo heeft het Cbp onder meer een adviserende taak bij de totstandkoming van nieuwe regelgeving. ACTAL is van mening dat gelet op de taken, bevoegdheden en kennis, het Cbp de aangewezen partij is om het bedrijfsleven bij te staan bij het voldoen aan de verplichtingen van de Wbp. Tegen deze achtergrond adviseert ACTAL het kabinet om het Cbp aan te sporen zijn meldingsformulieren in inhoud en vorm te vereenvoudigen en het elektronische meldingssysteem gebruiksvriendelijker te maken.

Voorzover het gaat om de uitvoeringskosten wordt als knelpunt genoemd dat de nulmetingen van de administratieve lasten van de Wbp door het Ministerie van Justitie te laag zijn ingeschat. Een ander knelpunt betreft de vergunningplicht voor doorgifte naar derde landen in de gevallen waar gebruik wordt gemaakt van door de Europese Commissie goedgekeurde modelcontracten. Ook de ingewikkeldheid van de meldingsformulieren en het gebruiksonvriendelijke elektronische meldingssysteem worden genoemd als knelpunten..

5.9 Technologie-onafhankelijkheid

In het voorgaande[475] is uiteengezet dat er vraagtekens worden gezet bij de technologie-onafhankelijkheid van de begrippen in de Wbp. Met name de invoering van RFID-toepassingen en het gebruik van het internet voor gegevensverwerkingen zou gevolgen hebben voor de privacywetgeving zoals wij die nu kennen. Te denken valt echter ook aan ontwikkelingen zoals biometrie en nanotechnologie.[476] Er is in de praktijk nog maar weinig praktische ervaring opgedaan met de toepassing van deze technologische ontwikkelingen. In paragraaf 5.2 noemden wij reeds enige voorbeelden rondom het gebruik van internet. Zo blijkt het in veel gevallen ondoenlijk om een verantwoordelijke aan te wijzen bij typische internetverschijnselen zoals weblogs, webfora en zoekmachines. Ook bestaat onduidelijkheid of internet service providers of internet access providers moeten worden aangemerkt als verantwoordelijke. Formeel-juridisch is de Wbp vaak wel van toepassing, maar feitelijk biedt de Wbp nauwelijks toegevoegde waarde in het reguleren van gegevensverwerkingen op internet.

---

[473] Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086 en Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
[474] VNO-NCW 2004.
[475] Zie par. 4.9 van dit rapport.
[476] Zie bijvoorbeeld: Marbus 2005, p. 57-61.

Winkelhorst[477] komt tot de conclusie dat de Wbp wel van toepassing kan zijn, maar niet uitgerust is om de dynamiek van de zoekmachines te kunnen normeren. Lodder e.a.[478] menen dat de Wbp onvoldoende houvast biedt om spam juridisch aan te pakken omdat de handhaving niet adequaat kan worden opgepakt door het feit dat de verzenders van spam zich veelal bevinden in landen waar de Wbp niet van toepassing is en zelfs als dit wel zo zou zijn, er maar beperkte mogelijkheden zijn om tegen de verzending van spam op te treden. En, zoals al aangegeven, stelt Zwenne[479] naar aanleiding van het Lindqvist-arrest dat de privacy-richtlijn veel minder technologieneutraal blijkt te zijn dan wel werd aangenomen.[480] Zwenne sluit daarmee niet uit dat er in de toekomst nog meer afstand zal worden genomen van het uitgangspunt dat de regelgeving zoveel mogelijk technologie-onafhankelijk moet zijn en dat dientengevolge de privacyregelgeving niet eenvoudiger wordt. De opmerking moet met name worden gezien tegen de achtergrond van de doorgiften naar derde landen, welke doorgiften in de praktijk zich toch met name voordoen in de private sector.

Er worden vraagtekens gezet bij de beoogde technologie-onafhankelijkheid van de Wbp. Verwerkingen die plaatsvinden met behulp van internet, het aanpakken van spam, de toepassing van biometrie en nanotechnologie lijken tegen toepassingsproblemen van de Wbp aan te lopen. De toepassing van de Wbp staat hier nog in zijn kinderschoenen. Het Lindqvist-arrest duidt op vragen met betrekking tot technologie-onafhankelijke benadering van de bescherming van persoonsgegevens.

5.10 Conclusies

Formeel-juridisch

De meest in het oog springende formeel-juridische knelpunten in de private sector doen zich met name voor rondom de interpretatie van (kern)begrippen en artikelen uit de Wbp. Deze knelpunten hebben ook gevolgen voor de aansluiting van het begrippenapparaat van de Wbp op aanverwante regelgeving zoals de Databankenwet en de Aanpassingswet inzake richtlijn elektronische handel. Daarnaast hebben deze knelpunten gevolgen voor de toepassing van de Wbp op internationale gegevensstromen, concernverhoudingen, fusies, overnames en het internet.

Een voorbeeld van een knelpunt betreft de afbakening van het begrip persoonsgegeven indien sprake is van foto- en beeldmateriaal. Zo zou op grond van dergelijke materiaal niet te snel moeten worden aangenomen dat er sprake is van persoonsgegevens omdat daarmee ook triviale zaken onderworpen zijn aan de strenge regels van de Wbp. Voorts zou niet elke handeling die met gegevens kunnen worden uitgevoerd, aangemerkt moeten worden als een verwerking. Met name valt hierbij te denken aan gevallen waarin gegevens slechts (technisch) worden bewaard of doorgegeven door een tussenpersoon of service provider.

Toepassing van het strikte kader van de Wbp leidt tot uitvoeringsproblemen bij internet gerelateerde gegevensverwerkingen, de bestrijding van spam en de toepassing van biometrie en nanotechnologie. Verder blijken verantwoordelijken moeilijk aan te wijzen bij gegevensverwerkingen die plaatsvinden door middel van het internet of gelijksoortige elektronische netwerksystemen. De Wbp is formeel-juridisch veelal van toepassing, maar mist de instrumenten om de dynamiek van deze gegevensverwerkingen te kunnen normeren en reguleren.

Een ander voorbeeld betreft de interpretatie van artikel 4 Wbp welk artikel ziet op de territoriale reikwijdte van de Wbp. De interpretatiemogelijkheden van dit artikel brengen knelpunten ten aanzien van de doorgifte problematiek met zich mee.

---

[477] Winkelhorst 2005, p. 146-154.
[478] Lodder e.a. 2004, p. 73.
[479] Zwenne 2004, p. 66-69.
[480] Bijv. *Kamerstukken II* 1997-98, 25 892, nr, 3, p. 41.

Naleving en handhaving

Het sectoroverstijgende karakter van de Wbp als omnibuswet heeft noodgedwongen geleid tot het formuleren van op onderdelen abstracte (open) normen in de Wbp. Een dergelijke abstractie leidt tot onduidelijkheid zoals bijvoorbeeld bij de verwerkingsgrondslagen 'toestemming' en 'gerechtvaardigd belang'. Dit heeft ook (in)directe gevolgen voor de mate waarin toegang tot gegevens door derden mogelijk is. Zo bestaat er een levendige handel in persoonsgegevens waarbij de afgelopen jaren excessen op een behoorlijke en zorgvuldige gegevensverwerkingen aan het licht zijn gekomen

Ook op andere fronten zijn er knelpunten naar voren gekomen rondom de naleving en handhaving van de Wbp. Zo leveren due diligence-onderzoeken een keur aan problemen met de Wbp op. De melding, de informatieplicht, het aanwezig zijn van een belang en het vragen van een vergunning, zijn normen die zich vaak slecht verdragen met het vertrouwelijke karakter van een overname. Verder willen verzekeraars meer toegang tot informatie die noodzakelijk is om de verzekeringsovereenkomst goed te kunnen uitvoeren en om verzekeringsfraude te voorkomen.

Zelfregulering is in de private sector langzaam van de grond gekomen. En ook rondom de melding en de vrijstelling daarvan is reeds sinds de invoering van de Wbp veel te doen. De melding zou eenvoudiger kunnen, vrijstellingen kunnen meer generiek worden en ook kan er op Europees niveau een standaardisering van de meldingsplicht worden bepleit voor ondernemingen met vestigingen in meerdere lidstaten van de Europese Unie. De informatieplicht kent veel open normen die in de praktijk tot rechtsonzekerheid leiden. Verduidelijking zou veel van die onzekerheid kunnen wegnemen. Voorts kan de jaarlijkse publicatieplicht omtrent de verstrekking aan derden van persoonsgegevens, worden afgeschaft zonder afbreuk te doen aan het beschermingsniveau van de betrokkene. De rechten van betrokkenen en dan met name het kennisnemingsrecht is voorwerp van veel geschillen. De rechtspraak hieromtrent is evenwel nog niet uitgekristalliseerd. De uitoefening van rechten door betrokkenen brengt lasten voor de verantwoordelijke met zich mee. Aan deze lasten kan tegemoet worden gekomen middels een hiertegenover staande (wettelijke) vergoeding. De inhoud en reikwijdte van deze vergoeding is echter nog onduidelijk.

Onduidelijk is wanneer de termijn aanvangt waarbinnen een betrokkene beroep kan instellen bij de rechtbank of bij het Cbp als de verwerking moet worden gestaakt zodra een betrokkene verzet heeft aangetekend tegen de verwerking voor commerciële of charitatieve doelen. Het stelsel van rechtsbescherming laat in civiele procedures een aantal belemmeringen zien rondom de toepassing van het burgerlijke procesrecht op de speciale procedures op grond van de Wbp. Het gaat dan vooral om een uniforme toepassing van het begrippenkader uit de Wbp en de toegankelijkheid van de burgerlijke rechter.

Ook de doorgiften laten veel problemen zien die zich in de dagelijkse praktijk voordoen bij ondernemingen. Zo zorgt de vergunningplicht bij het gebruik maken van modelcontracten voor ergernis en bestaat onduidelijkheid over de toepassing van de uitzonderingsgronden op basis waarvan een doorgifte toch mogelijk is zonder vergunning. Een due diligence-onderzoek bij een overname stuit ook op problemen door de restrictieve benadering van de wetgever en de toezichthouder. Voorts wordt opgemerkt dat het stelsel rondom de doorgiften niet consistent is. Ook doorgiften waarvoor bijvoorbeeld geldt dat de Wbp van toepassing is en zorgt voor een passend beschermingsniveau, kunnen onderworpen zijn aan de wettelijke plicht om nog een vergunning aan te vragen.

Beeldvorming en bekendheid

Bekendheid met de rechten en plichten van de Wbp is van belang voor het creëren van draagvlak voor de bescherming van persoonsgegevens. Op verschillende rechtsgebieden binnen de private sector zoals in het arbeidsrecht en het financieel recht, komt naar voren dat de bekendheid met de Wbp bij civiele rechters beperkt lijkt. Voor zover er al een tendens lijkt waar te nemen dat hier op sommige gebieden verandering in komt, verloopt die ontwikkeling langzaam.

Ten aanzien van de bekendheid met de Wbp laat vooral het burgeronderzoek door TNS NIPO[481] zien dat veel burgers niet op de hoogte zijn van de Wbp en/of diens toezichthouder. Burgers lijken evenwel veel belang te hechten aan een bescherming van persoonsgegevens. Het grootste vertrouwen wordt daarbij gesteld in de overheid. Bedrijven zouden volgens het opinierapport meer aandacht van het Cbp mogen krijgen dan de overheid.

De beginselen van de Wbp zoals transparantie en zelfbeschikking komen met name in het gedrang als het schort aan bekendheid met de Wbp. Verder kan uit de eerder gesignaleerde knelpunten dat er sprake is van onduidelijkheid bij de toepassing van de Wbp als gevolg van het gebruik van abstracties en open normen, worden afgeleid dat dit leidt tot een negatieve beeldvorming. Niet alleen van de Wbp zelf, maar ook ten aanzien van de bescherming van persoonsgegevens en daarmee de waarborging van de grondrechten van burgers.

[481] Schildmeijer, Samsons & Koot 2005.

Hoofdstuk 6: Publieke sector

6.1 Inleiding

In dit hoofdstuk wordt per thema ingegaan op de belangrijkste en meest in het oog springende knelpunten in de publieke sector die zijn gesignaleerd in de literatuur. Tot de publieke sector rekenen wij onder meer de ministeries, provincies, gemeenten en waterschappen, openbare lichamen en zelfstandige bestuursorganen met rechtspersoonlijkheid die bij of krachtens de wet zijn ingesteld. Het is onvermijdelijk dat er overlap bestaat tussen de in dit hoofdstuk gesignaleerde knelpunten en knelpunten die in het algemene en in de overige sectorspecifieke hoofdstukken zijn beschreven. Deze knelpunten worden in dit hoofdstuk toch kort genoemd omdat deze specifiek voor de publieke sector bepaalde consequenties hebben, of omdat het nuttig lijkt om ze te illustreren aan de hand van specifieke voorbeelden uit de publieke sector waaronder jaarverslagen van verschillende functionarissen voor de gegevensbescherming. Als het aan de orde is, zal dat kort worden toegelicht

6.2 Werkingssfeer en toepassing

Hoewel niet specifiek voor de publieke sector blijken uit literatuuronderzoek vooral onduidelijkheden rond de uitleg en toepassing van begrippen van de Wbp zoals 'persoonsgegevens' en 'verantwoordelijke'. Dit kan consequenties hebben voor de doeltreffendheid van de Wbp, nu het begrip persoonsgegevens zo'n centrale rol speelt in de wet en het object van bescherming vormt. Voor de publieke sector kan dit worden geïllustreerd met een aantal voorbeelden. Ook bestaat binnen de publieke sector onduidelijkheid over de verhouding van de Wbp met andere specifieke wetten.

6.2.1 Begrippen

Het blijkt lastig te zijn te bepalen wie in de praktijk verantwoordelijk is voor het daadwerkelijk naleven van de materiële normen van de Wbp. Schreuders en Gardeniers[482] schetsen twee situaties ter illustratie. Als eerste wordt de situatie geschetst waarin het bestuursorgaan in de praktijk geen of nauwelijks feitelijke bemoeienis heeft of hoeft te hebben met het verwerken van persoonsgegevens. Bij ministeries en gemeenten bijvoorbeeld, zijn de minister respectievelijk het college van B&W de verantwoordelijke voor alle verwerkingen van persoonsgegevens. Vanzelfsprekend zullen en kunnen zij persoonlijk geen feitelijke of praktische invulling geven aan deze verantwoordelijkheid. Schreuders en Gardeniers werpen daarom de vraag op of de Wbp niet ook een voorziening zou moeten bevatten ten aanzien van het verplicht aanwijzen van een beheerder en het beleggen van de bijbehorende verantwoordelijkheden in de praktijk van respectievelijk ministeries en gemeenten. Uit privacyjaarverslagen van ministeries blijkt dat ook zonder dat dit verplicht is, vooral grote organisaties beheerders benoemen en aan hen bijbehorende verantwoordelijkheden, taken en bevoegdheden toedelen. Een tweede situatie waarin het volgens Schreuders en Gardeniers vaak niet eenvoudig is om de verantwoordelijke vast te stellen, is die waarbij sprake is van samenwerking tussen organisaties, al dan niet door middel van samenwerkingsverbanden. Een sociale dienst van een gemeente werkt bijvoorbeeld nauw samen met de Belastingdienst en de politie bij de aanpak van georganiseerde criminaliteit. In een dergelijk samenwerkingsverband is het lastig om een verantwoordelijke te identificeren voor de gegevens die in het kader van de samenwerking worden verwerkt en gedeeld. Onder meer om deze reden heeft het Cbp een informatieblad uitgegeven over de wijze waarop in dergelijke sa-

[482] Schreuders & Gardeniers 2005, p. 260-261.

menwerkingsverbanden met persoonsgegevens dient te worden omgegaan.[483] Daarin wordt ondermeer aandacht besteed aan de onduidelijkheden rond het aanwijzen van verantwoordelijken.

6.2.2 Toepassing

Ook voor de publieke sector geldt dat toepassing van de regels en normen uit de Wbp bepaald geen sinecure blijkt. De beantwoording van de vraag of de Wbp van toepassing is en of de gegevensverwerking de toets van de Wbp kan doorstaan ligt in eerste instantie bij de verantwoordelijke Als het gaat om de verwerking van gegevens in de gemeentepraktijk concludeert van Pomeren[484] in een speciaal aan dit onderwerp gewijd artikel in de Gemeentestem dat:

> '[d]ie beoordeling niet altijd eenvoudig [is] te maken'

Dat wordt veroorzaakt door de open en vage normen in de wet, zoals in het voorgaande uiteengezet in hoofdstuk 4. Daarnaast heeft een verantwoordelijke binnen de publieke sector niet alleen te maken met de Wbp, maar ook met tal van specifieke regelingen die ook zien op de verwerking van persoonsgegevens. Van Pomeren wijst, evenals Cuipers,[485] in dit verband op de wat onduidelijke verhouding tussen de Wbp en de Wob. Ook Overkleeft-Verburg[486] waarschuwt voor mogelijke problemen die de samenloop van de Wob en de Wbp kunnen veroorzaken:

> 'Er zijn casusposities denkbaar, waarin niettemin problemen zouden kunnen ontstaan, met name door het (partiële) verschil in beschermingsniveau van de rechten op privacy en gegevensbescherming en de specifieke uitleg die de Afdeling bestuursrechtspraak in het kader van de Wob aan de persoonlijke levenssfeer als weigeringsgrond geeft. Werkelijke problemen zijn in de uitvoeringspraktijk echter nog niet gesignaleerd.'

Van Pomeren wijst verder op de verhouding tussen de Wbp en de Wet Bevordering integriteitbeoordelingen door het openbaar bestuur (Wet Bibob). De verhouding met specifieke regelingen voor de verwerking van persoonsgegevens door de publieke sector levert onduidelijkheid op. Denk bijvoorbeeld aan de Wet Gemeentelijke Basisadministratie (WGBA) en de Wet op de Inlichtingen en Veiligheidsdiensten 2002 (WIV2002), de Wet politieregisters (WPolr, straks de Wet politiegegevens WPolg), de Wet justitiële en strafvorderlijke gegevens (WJSG). Nieuwe ontwikkelingen die discussie oproepen, bijvoorbeeld het Burger Service Nummer[487], worden in een aparte wettelijke regeling opgenomen. Zodoende wordt de discussie in eerste instantie vooral buiten het Wbp-kader gevoerd.[488]

Daarmee is een aantal risicovolle gebieden op voorhand buiten de werkingssfeer van de Wbp gehouden. Daarin kan een oorzaak worden gevonden voor het relatief geringe aantal knelpunten dat in literatuur naar voren is gekomen als het gaat om het gebruik van persoonsgegevens binnen de publieke sector. Dat betekent echter niet dat de Wbp helemaal niet van toepassing is. Het Cbp adviseert over nieuwe wetgeving op basis van het normenkader van de Wbp en geeft daarbij vaak wijzigingsvoorstellen of richtingen om nieuwe wetgeving meer in overeenstemming met de Wbp te brengen. [489] Op die manier wordt op een bepaald deelgebied invulling gegeven aan de open en vage normen uit de Wbp. Is in een wettelijke regeling geen

---

[483] Cbp, mei 2005, informatieblad 31A.
[484] Van Pomeren 2006, p. 333.
[485] Cuipers 2004, p. 346-350.
[486] ABRvS 8 december 2004, *JB* 2005/26 m.nt. G. Overkleeft-Verburg; ABRvS 15 juni 2005, *JB* 2005/230, m.nt. G. Overkleeft-Verburg; ABRvS 14 juli 2004, *JB* 2004/297, m.nt. G. Overkleeft-Verburg.
[487] *Kamerstukken II* 2005-2006, 30 312.
[488] Zie bijvoorbeeld Cbp Advies aan de leden van de Vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties 25 oktober 2005, z2005-1198; Cbp Advies aan Minister van Bestuurlijke Vernieuwing en Koninkrijkrelaties, 10 februari 2005, z2004-1734.
[489] Zie bijvoorbeeld Cbp, Brief 12 juli 2006, z2006-0683.

nadere invulling gegeven aan de regels en normen uit de Wbp dan acht het Cbp de Wbp logischerwijs onverkort van toepassing.[490]

In de publieke sector bestaan onduidelijkheden over de uitleg en toepassing van begrippen als verantwoordelijke en persoonsgegeven alsmede over de verhouding met andere wetten, zoals de Wob en de Wet Bibob.

6.3 Normatieve kaders

Zoals aangegeven in hoofdstuk 4 worden ook in het domein van de publieke sector knelpunten gesignaleerd op het gebied van de interpretatie van open normen, de deskundigheid die nodig is om de wet toe te kunnen passen, en het verbod van het verwerken van bijzondere gegevens in specifieke gevallen. Vragen die specifiek raken aan het thema privacy en veiligheid zijn geen onedrwrep van dit onderzoek. Wel wordt in dit hoofstuk kort ingegaan op het verwante thema 'openbare orde' waar zich dergelijke knelpunten voordoen, op het verbod van verwerken van bijzondere gegevens en situaties waarin dat een knelpunt kan opleveren en op het fenomeen samenwerkingsverbanden.

6.3.1 Openbare orde

Een belangrijke taak binnen de publieke sector is de handhaving van de openbare orde. Dat is voor een deel een taak die ondersteund wordt door gegevensverwerkingen die buiten het werkingsgebied van de Wbp liggen. Denk daarbij aan de gegevensverwerkingen die door politie, justitie en bijvoorbeeld de Algemene Inlichtingen- en Veiligheidsdienst worden gevoerd. Daarnaast is er een aantal ontwikkelingen waarneembaar, waarbij initiatieven van overheidsinstanties te maken krijgen met het normenkader uit de Wbp. Het gaat dan vooral om samenwerkingsverbanden tussen verschillende (overheids)instanties. In sommige gevallen staat de Wbp aan de uitvoering van bepaalde vormen en wijzen van samenwerking in de weg.

Een voorbeeld hiervan is de wijze waarop de gemeente Heerlen het tippelverbod uit de Algemene Plaatselijke Verordening (APV) wilde handhaven. Het ging specifiek om de aanpak van prostitutie door op grond van de APV dwangsommen op te leggen aan overtreders. De gemeente wenste daarvoor de kentekenadministratie van de Dienst Wegverkeer (RDW) te gebruiken. Het RDW weigerde. Tijdens de bezwaarprocedure hebben de gemeente Heerlen en de RDW de casus voor nader onderzoek aan het Cbp voorgelegd. Het Cbp kon zich vinden in de afweging die de RDW had gehanteerd.[491] De afweging van de RDW hield in dat binnen de wegenverkeerswetgeving ruimte bestaat om in de in deze regelgeving bepaalde gevallen, aan bepaalde instanties gegevens te verstrekken. De gemeente behoorde echter niet tot de instanties die genoemd werden in de wetgeving. Het Cbp voegde daar aan toe dat ook artikel 9 van de Wbp geen oplossing bood vanwege de context van de gegevensverstrekking, en dat onvoldoende maatregelen waren getroffen om eventuele gevolgen van onterechte conclusies te voorkomen of te herstellen. Het Cbp oordeelde verder dat de verwantschap tussen het doel van de Wegenverkeerswet en de verstrekkingsgrond zeer (te) klein was.

Een landelijke tendens als het gaat om openbare veiligheid is de opkomst van cameratoezicht ter bevordering van de veiligheid in de openbare ruimten. Voor de toepassing ervan is een grondslag gecreëerd in de Gemeentewet (Gw). Het Cbp heeft een aflevering uit de reeks 'Achtergrondstudies en Verkenningen' aan het onderwerp cameratoezicht gewijd.[492] In die aflevering heeft het Cbp een aantal vuistregels gegeven voor de inrichting en besluitvorming ten aanzien van cameratoezicht in het publieke domein. De publiek-

[490] Zie bijvoorbeeld Cbp Advies aan Staatssecretaris van Financiën, 16 maart 2005, z2005-0126.
[491] Cbp Uitspraak 29 oktober 2001, z2001-0503.
[492] Smeets 2004.

rechtelijke taak op basis van de Gw dient als grondslag voor de rechtmatigheid van de verwerking op grond van de Wbp. De Wbp is op het cameratoezicht volledig van toepassing, wat inhoudt dat betrokkenen op hun (inzage) rechten moeten worden gewezen, dat het cameratoezicht alleen voor het vooraf bepaalde doel mag worden ingezet en voldoende moet zijn beveiligd. Ook mogen de beelden niet langer worden bewaard dan strikt noodzakelijk is.

Een belangrijke constatering in dit verband komt van Holvast, Merkus en Michels.[493] Daar waar echte bescherming nodig is, 'regeert de strijd tegen het terrorisme, de fraude en de criminaliteit en worden Richtlijn en wet simpelweg terzijde geschoven', zo stellen zij.

6.3.2 Bijzondere gegevens

Het verbod tot het verwerken van bijzondere gegevens kan knelpunten opleveren in geval van verificatieonderzoek en nalevingsonderzoek. Dat is ook door het Cbp in een brief aan de Minister van Justitie geconstateerd. Een concreet knelpunt dat wordt genoemd is het onderzoek door accountants en auditors bij bijvoorbeeld gemeenten. Accountants en auditors hebben op dit moment niet de mogelijkheid om inzage te krijgen in bestanden die bijzondere persoonsgegevens bevatten. Het verbod op het verwerken van bijzondere gegevens uit artikel 16 Wbp staat hieraan in de weg. Accountants hebben deze mogelijkheid nodig voor bijvoorbeeld controle van de 'zorgzwaarte' van thuiszorg en WVG-verstrekkingen[494] door gemeenten. Het Cbp is van oordeel dat accountants en auditors daar waar dat daadwerkelijk noodzakelijk is voor de uitvoering van hun taak (steekproefsgewijs) bijzondere gegevens moeten kunnen verwerken. Het Cbp voegt daar aan toe dat dit wel een laatste middel dient te zijn. Ook de Nationale Ombudsman heeft het Cbp laten weten problemen te ervaren bij het beschikbaar komen van bijzondere gegevens tijdens zijn onderzoeken. Het Cbp heeft in een brief de Minister van Justitie in overweging gegeven te bezien of deze problematiek opgelost kan worden met een algemene ontheffingsgrond in de Wbp, een regeling in de Awb en/of aanpassing van bijzondere wetten.[495]

6.3.3 Samenwerkingsverbanden

In de praktijk bestaat een vrij hardnekkig beeld dat privacywetgeving de uitwisseling van gegevens in samenwerkingsverbanden hindert, met name die in de publieke sector. Het gaat dan vooral om de voorkoming van overlast en de bevordering van de veiligheid. De burgemeester van Rotterdam, Opstelten, stelde in 2002 dat privacywetgeving de aanpak van overlast belemmert. Aanpassing van privacywetgeving stond hoog op de lijst van 'Tien punten voor een veilige stad' die hij presenteerde aan de vaste kamercommissies voor Binnenlandse Zaken en Koninkrijksrelaties en voor Justitie. Het Cbp bleek het hiermee niet eens.[496] Het blijkt echter een hardnekkig beeld te zijn. Ook tijdens een bijeenkomst georganiseerd door het Cbp, kwam het beeld naar voren dat privacywetgeving de gegevensuitwisseling in samenwerkingsverbanden in de weg staat. Het Cbp bestreed dat beeld en stelde dat privacywetgeving samenwerkingsverbanden niet verbiedt, maar slechts randvoorwaarden aan een dergelijke verwerking stelt.[497]

---

[493] Holvast, Merkus & Michels 2004, p. 249.
[494] WVG staat voor Wet Voorzieningen Gehandicapten(zorg).
[495] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
[496] Cbp Advies aan Burgermeester van Rotterdam, 27 november 2002, z2002-1335.
[497] Cbp, Mededeling 24 mei 2005.

In de publieke sector doen zich knelpunten voor ten aanzien van het verbod van verwerken van bijzondere gegevens, specifiek als het gaat om het controleren van de naleving van wetgeving, waarvoor bijzondere gegevens als gezondheidsgegevens worden bijgehouden. Ook kunnen zich knelpunten voordoen bij het verwerken van persoonsgegevens in samenwerkingsverbanden. Het Cbp geeft echter aan dat dat niet (altijd) het geval hoeft te zijn. De Wbp zou slechts randvoorwaarden stellen aan dergelijke verwerkingen in samenwerkingsverbanden.

6.4 Zelfregulering

In deze paragraaf wordt ingegaan op gedragscodes of liever gezegd, het ontbreken daarvan in de publieke sector, op informele zelfregulering en op de functionaris voor de gegevensbescherming.

6.4.1 Gedragscodes

Er zijn geen (formele) gedragscodes in de publieke sector bekend die op grond van artikel 25 en 26 Wbp tot stand zijn gekomen. Dit heeft mede zijn invloed op literatuur, waar slechts zeer beperkt op het punt van zelfregulering wordt ingegaan. Het feit dat er geen gedragscodes in de publieke sector bekend zijn, kan er mee te maken hebben dat de overheid altijd rekening dient te houden met het legaliteitsbeginsel en dat haar handelen altijd gebaseerd moet zijn op wet- en regelgeving. Voor normering van het overheidshandelen is veelal in verschillende sectoren sectorale wetgeving tot stand gekomen, zoals behandeld in paragraaf 6.2.2.

6.4.2 Informele zelfregulering

Hoewel er geen formele gedragscodes bekend zijn, is er wel een andere vorm van zelfregulering aanwezig. Met de term 'informele zelfregulering' wordt een vorm van zelfregulering bedoeld waarbij geen goedkeuring van het Cbp is gevraagd of gekregen en zodoende niet kan worden gesproken van een gedragscode in de zin van de Wbp. Daarnaast kan deze status er veelal niet aan worden gegeven, omdat de vorm van informele zelfregulering niet voor een gehele sector van toepassing is. Verschillende publieke organisaties vormen informele netwerken of platforms[498], waarbinnen zogenaamde best practices, maar ook uitwerkingen van de Wbp in concrete modellen, protocollen of andere afspraken, worden ontwikkeld. Deze modellen, protocollen of andere afspraken hebben geen formele status, maar hebben wel een uniforme toepassing, naleving en controle van de naleving van de Wbp tot gevolg. Ook kan bijvoorbeeld gedacht worden aan het instrument van circulaires waarin afspraken worden neergelegd met betrekking tot gegevensuitwisseling met de publieke sector.[499]

6.4.3 Functionaris voor de gegevensbescherming

Opgemerkt wordt dat er een groot aantal functionarissen voor de gegevensbescherming actief is binnen de publieke sector. Blijkens het openbaar register bij het Cbp, zijn een groot aantal opgaven van functionarissen gegevensbescherming gedaan door publieke organisaties. Ook is er een vereniging voor overheidsfunctionarissen voor de gegevensbescherming.[500] Dat deze functionarissen voor de gegevensbescherming

[498] Zoals bijvoorbeeld het geval is in de onderwijssector. Zie het jaarverslag van de privacyfunctionaris van het Ministerie van OCW.

[499] Het Cbp oordeelde negatief over een concept-circulaire gegevensuitwisseling van de SVB: Cbp Advies aan Staatssecretaris SZW, 30 maart 2004, z2004-0058.

[500] Zie het jaarverslag 2003 van de privacyfunctionaris van het Ministerie van VROM, p. 18.

ook actief zijn blijkt bijvoorbeeld uit een contactdag voor deze functionarissen bij gemeenten die in 2003 is georganiseerd, waarbij kennis en ervaringen werden uitgewisseld.[501]

De functionaris voor de gegevensbescherming houdt toezicht op de naleving van de Wbp. Uit een aantal jaarverslagen[502] van de functionarissen komt naar voren dat naleving van de Wbp een aanzienlijke inspanning vergt. Deze inspanning wordt vergroot daar waar de naleving van de Wbp gekoppeld wordt aan het onderwerp informatiebeveiliging. Een dergelijke koppeling is vaak dermate complex dat dit externe beoordelingen vraagt van specialisten. De jaarverslagen schetsen verder dat privacybewustzijn een sterk bepalende factor is voor de mate waarin de Wbp wordt nageleefd. Daar schort het echter nog vaak aan, ondanks de inspanningen van de functionarissen. Reeds het bewustzijn alleen, vormt een voortdurend en aanzienlijk tijdintensief punt van aandacht voor de functionarissen. Een ander knelpunt is dat functionarissen veelal niet de bevoegdheden door de verantwoordelijke toegekend krijgen, waar zij op grond van de Wbp recht op zouden hebben. Veel verantwoordelijken blijken vaak niet de juiste bevoegdheden te kunnen toekennen uit onbekendheid met de Wbp.

In de publieke sector zijn relatief veel functionarissen voor de gegevensbescherming aangesteld. Er zijn geen gedragscodes bekend, maar wel doen zich verschillende vormen van informele zelfregulering voor die een uniforme toepassing, naleving en controle van de naleving bevorderen. Uit de jaarverslagen blijkt dat het toezicht op naleving en het stimuleren van het bewustwordingsproces veel inspanning vergt.

6.5 Transparantie en rechten van betrokkenen

Eén van de beginselen van de Wbp is transparantie van gegevensverwerking. Transparantie houdt in dat betrokkenen moeten kunnen weten welke verantwoordelijke, voor welke doeleinden, welke persoonsgegevens, over hem of haar verwerkt. Pas dan zijn betrokkenen in staat effectief van hun rechten gebruik te maken. Hiertoe zijn in de Wbp de meldingsplicht, de informatieplicht en het inzage- en correctierecht opgenomen. Op basis van literatuur komen de volgende knelpunten bij de toepassing van deze artikelen naar voren.

6.5.1 Kennisnemingsrechten van betrokkenen

Uit de verschillende jaarverslagen van functionarissen voor de gegevensbescherming komt een beeld naar voren dat de betreffende organisaties veelal niet zijn voorbereid op het gevolg geven aan de uitoefening van rechten van betrokkenen zoals het kennisnemingsrecht. Zo doet de functionaris voor de gegevensbescherming van het Ministerie van VROM pas in het jaarverslag 2003 de aanbeveling om op korte termijn een procedure vast te stellen waardoor de rechten van betrokkenen worden gewaarborgd binnen de organisatie.[503] Vaak ontbreekt het in organisaties aan procedures en maatregelen die er voor moeten zorgen dat een betrokkene binnen vier weken een reactie van de verantwoordelijke krijgt op zijn verzoek(en). Tot nog toe heeft dat in de praktijk niet tot knelpunten geleid, maar dat lijkt meer te wijten aan de vooralsnog weinige verzoeken die door betrokkenen worden gedaan.[504] De gemeente Best heeft bijvoorbeeld in 2005

[501] Cbp, Mededeling 15 september 2003.

[502] Jaarverslag FG Gemeente Arnhem 2005, Jaarverslag FG Gemeente Best 2005, Jaarverslag FG Inlichtingenbureau 2005, Jaarverslag FG Ministerie van VROM 2003 & 2004, Jaarverslag FG Ministerie van LNV, 2003/2004, Jaarverslag FG Ministerie van EZ 2003 en Jaarverslag FG Ministerie van VWS 2003.

[503] Zie het jaarverslag FG Ministerie van VROM, p. 7.

[504] Jaarverslag FG Gemeente Arnhem 2005, Jaarverslag FG Gemeente Best 2005, Jaarverslag FG Inlichtingenbureau 2005, Jaarverslag FG Ministerie van VROM 2003 & 2004, Jaarverslag FG Ministerie

geen enkel verzoek gekregen en de gemeente Arnhem in 2003 slechts drie. Ook in de bijeenkomst met domeindeskundigen gaven de meeste aanwezigen aan dat in hun organisatie maar weinig verzoeken tot inzage of correctie werden gedaan. Het Ministerie van Buitenlandse Zaken vormde hierop een uitzondering. Advocaten van asielzoekers blijken nogal eens een beroep te doen op het kennisnemingsrecht. Weliswaar voor procedurele doeleinden maar wel zodanig veel dat het ministerie hiervoor substantiële capaciteit heeft moeten vrijmaken.

Overkleeft-Verburg[505] wijst in een noot onder een uitspraak van de Afdeling bestuursrechtspraak op het te gemakkelijk wegschrijven van het correctierecht door de Afdeling en de daarmee gepaard gaande 'falende rechtsbescherming'. Publieke registraties, in dit geval het kentekenregister van de RDW, hebben een belangrijke functie in de uitvoering van publieke taken. Toenemende indentiteitsfraude brengt daarbij extra risico's mee voor betrokkenen om geconfronteerd te worden met de gevolgen van een foutieve registratie in een dergelijk register. In het voorkomen of oplossen daarvan zou de aanvullende waarborgende werking van het correctierecht beter benut moeten worden.

De potentiële kracht van het kennisnemingsrecht blijkt uit een gegevensverwerking door de gemeente Nijmegen in het kader van het 'Digitaal Bouwarchief'. Naar aanleiding van een aantal bezwaren van betrokkenen heeft de gemeente het systeem in overeenstemming met de Wbp gebracht.[506] Daartegenover staat dat ook binnen de publieke sector verwarring kan ontstaan over de uitoefening van deze rechten. Zo bestond bij een betrokkene die inzage vorderde in de op haar betrekking hebbende dossiers bij de commissie van advies voor de bezwaar- en beroepschriften van een gemeente, verwarring over de forumkeuze. De betrokkene heeft een procedure op basis van artikel 46 Wbp gestart, om een jaar later in hoger beroep te horen dat zij gebruik had moeten maken van artikel 45 Wbp en de bestuursrechtelijke weg had moeten bewandelen. Het Hof bepaalde een nieuwe termijn voor de behandeling van het bezwaarschrift.[507]

6.5.2 Informatieplichten voor verantwoordelijken

Uit verschillende jaarverslagen van functionarissen voor de gegevensbescherming blijkt dat er aandacht is voor het naleven van de informatieplicht. Zo vraagt de functionaris van het Ministerie van VROM in zijn jaarverslag van 2004 aandacht voor een ministeriebrede procedure, maar merkt daarbij tegelijkertijd op dat binnen een aantal organisatie-onderdelen is voorzien in zo'n procedure. Uit de bestudeerde literatuur en jurisprudentie komen evenwel geen duidelijke knelpunten ten aanzien van de naleving van de informatieplicht naar voren.

6.5.3 Meldingen

Uit de jaarverslagen van functionarissen voor de gegevensbescherming van diverse ministeries kan worden afgeleid dat ministeries over het algemeen aan de meldingsplicht voldoen, althans, de intentie hebben om daar op een zorgvuldige wijze aan te voldoen. Uit deze jaarverslagen kan worden opgemaakt dat gegevensverwerkingen nauwkeurig worden geïnventariseerd en beoordeeld. In 2004 heeft het Ministerie van VROM bijvoorbeeld 252 verwerkingen van persoonsgegevens gemeld, het Ministerie van EZ heeft in 2002 in totaal 254 verwerkingen van persoonsgegevens geïnventariseerd, waarvan er 61 zijn gemeld bij het

---

van LNV, 2003/2004, Jaarverslag FG Ministerie van EZ 2003 en Jaarverslag FG Ministerie van VWS 2003.

[505] ABRvS 7 december 2005, *LJN* AU7614, *JB* 2006, 50 m.nt. G. Overkleeft-Verburg.

[506] Cbp Uitspraak 1 december 2005, z2005-0212.

[507] Gerechtshof Leeuwarden 4 december 2002, *LJN* AF1344.

Cbp, en het Ministerie van VWS heeft in 2002 in totaal 331 verwerkingen geïnventariseerd, waarvan er 111 meldingsplichtig waren.[508]

Gemeenten leken in de eerste jaren onder het regime van de Wbp in veel mindere mate aan de meldingsplicht te voldoen. Het Cbp heeft in 2003 een lijst gepubliceerd van gemeenten die niet aan de meldingsplicht hadden voldaan. Ook heeft zij veertien gemeenten hard aangepakt wegens het niet voldoen aan de meldingsplicht. Zo hebben onder meer de gemeente Best, Hellevoetsluis, Horst aan de Maas, en Kampen, boetes opgelegd gekregen. Daarbij was de gemeente Best in eerste instantie het zwaarst beboet met een boete van €15.000.

Een belangrijk (inmiddels door de wetgever verholpen) knelpunt vormde de bevoegdheid van het Cbp tot het opleggen van boetes voor verwerkingen van persoonsgegevens die niet waren gemeld in het openbaar register bij het Cbp maar al wel bestonden op 1 september 2001 (datum inwerkingtreding Wbp).[509] De Afdeling bestuursrechtspraak bepaalde dat er geen boetebevoegdheid bestaat bij gegevensverwerkingen die al bestonden bij inwerkingtreding van de Wbp. De gemeente Best had bijvoorbeeld een boete opgelegd gekregen vanwege het te laat voldoen aan de meldingsplicht van artikel 27 lid 1 van de Wbp. Het bezwaarschrift hiertegen was door het Cbp ongegrond verklaard. Ook de rechtbank 's-Hertogenbosch had het beroepschrift ongegrond verklaard.[510] De boetebeschikking werd echter door het Cbp als gevolg van de uitspraak van de Afdeling Bestuursrechtspraak weer ingetrokken, en de boete van € 15.000 teruggestort naar de gemeente Best. Inmiddels is dit knelpunt gerepareerd door de wetgever.[511]

Een ander knelpunt dat is geconstateerd door het Cpb betreft de handhaving van de meldingsplicht. Bij overtreding van de verplichting om een verwerking van persoonsgegevens te melden bij het Cbp of een functionaris voor de gegevensbescherming, kan het Cbp op grond van artikel 66 Wbp een bestuurlijke boete opleggen van ten hoogste € 4.500. Het in artikel 75 lid 1 en lid 2 van de Wbp als misdrijf gekwalificeerde strafbare feit van opzettelijk niet melden wordt bedreigd met gevangenisstraf of een geldboete van de derde categorie. Het Cbp constateert dat daarmee de maximale bestuurlijke boete twee keer zo hoog is als de maximale strafrechtelijke boete van € 2.250. Deze situatie acht het Cbp onwenselijk.[512]

Met betrekking tot het Vrijstellingsbesluit merkt Holvast op dat zelfs bij het voldoen aan alle voorwaarden, de vrijstelling geen 'echte' vrijstelling van de meldingsplicht hoeft te zijn. Zo schrijft artikel 30 lid 3 Wbp voor dat elke verantwoordelijke die gebruikmaakt van het Vrijstellingsbesluit, desgevraagd inlichtingen moet verstrekken over de door hem verwerkte persoonsgegevens. De auteur werpt hiermee de vraag op of daarmee de beoogde transparantie of bewustwording wel wordt bereikt. Tijdens de bijeenkomst met domeindeskundigen gaf een functionaris voor de gegevensbescherming aan dat in zijn ministerie alle verwerkingen worden geïnventariseerd en bij hem gemeld, omdat het inzicht in en overzicht van alle verwerkingen van persoonsgegevens toch nodig is. Alle verwerkingen van persoonsgegevens moeten immers aan de Wbp voldoen, en niet alleen de meldingsplichtige. Uit jaarverslagen van andere ministeries blijkt dat ook andere ministeries alle gegevensverwerkingen inventariseren en beoordelen, en niet alleen de meldingsplichtige. Dit hoeft op zichzelf geen knelpunt te zijn. Echter, de wetgever heeft met de vrijstellingsmogelijkheid beoogd de administratieve lasten van de wet te verlichten. Voor de administratieve lasten die met de feitelijke naleving van de Wbp gemoeid zijn, lijkt het Vrijstellingsbesluit nauwelijks verschil te maken.

---

[508] Zie de eerder aangehaalde jaarverslagen.
[509] ABRvS 21 september 2005, *LJN* AU2998, *JB* 2005, 292, m.nt. G. Overkleeft-Verburg.
[510] Rechtsbank 's–Hertogenbosch 18 januari 2005, *LJN* AT0462.
[511] *Stb.* 2006, 24 en *Stb.* 2006, 196.
[512] Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494.

Van het kennisnemings- en correctierecht wordt in de publieke sector in het algemeen niet veel gebruik gemaakt. Er zijn aanwijzingen dat procedures en maatregelen vaak ontbreken om deze rechten binnen de wettelijke termijnen op een zorgvuldige wijze te kunnen effectueren. De meldingsplicht zal bijdragen aan de transparantiedoelstelling van de wet, maar nauwelijks aan de doelstelling van administratieve lastenverlichting.

6.6 Toezicht en rechtsbescherming

Toezicht kan worden uitgeoefend door het Cbp, de functionaris gegevensbescherming en het Ministerie van Justitie. De rechtsbescherming tegen besluiten door verantwoordelijken uit de publieke sector, die als bestuursorganen in de zin van de Awb kunnen worden gekwalificeerd, wordt bepaald door diezelfde Awb. Hieronder wordt op gesignaleerde knelpunten in het toezicht en de rechtsbescherming ingegaan.

6.6.1 Toezicht door het Cbp

Het Cbp kan op verschillende wijzen toezicht uitoefenen, namelijk door ambtshalve of klachtonderzoek (art. 60 Wbp), door voorlichting (art. 51 Wbp), door bemiddeling in geschillen (art. 47 Wbp) of door een voorafgaand onderzoek (art. 31 Wbp). Onderdeel van de uitoefening van het toezicht is ook de organisatorische uitvoering van de toezichtstaak en de scheiding tussen de wettelijke taak van het Cbp en de Minister van Justitie. De functionaris voor de gegevensbescherming fungeert als interne toezichthouder van een verantwoordelijke. Ook de functionaris komt dientengevolge bepaalde bevoegdheden toe. De functionaris is hierboven in paragraaf 6.4.3 al even aan de orde geweest.

Eén van de knelpunten die wordt genoemd in literatuur betreft de doorlooptijd van het voorafgaand onderzoek door het Cbp. In dat kader geeft Van Schoonhoven het voorbeeld van de veelvuldig voorkomende praktijk waarin sprake is van samenwerkingsverbanden tussen organisaties in de publieke sector en/of private sector. Vaak is deze samenwerking noodzakelijk om maatschappelijke problemen aan te pakken waarbij binnen het samenwerkingsverband informatie wordt gedeeld die onder de reikwijdte van artikel 31 Wbp valt en waarvoor dus een voorafgaand onderzoek door het Cbp is vereist. Voor de verantwoordelijke geldt dat het aanvragen en doorlopen van de procedure van het voorafgaand onderzoek wettelijk noodzakelijk is, maar een vertragende werking kan hebben op het voortvarend kunnen oppakken van de maatschappelijk gewenste werkzaamheden door het samenwerkingsverband.

Wettelijk gezien mogen er pas persoonsgegevens worden uitgewisseld als het Cbp heeft verklaard dat deze verstrekking rechtmatig is. Een voorafgaand onderzoek door het Cbp kan gelet op de huidige wettelijke termijnen, echter maximaal 24 weken duren nu per 1 juli 2005 de uniforme openbare voorbereidingsprocedure van de Awb is gewijzigd.[513] De mogelijk lange doorlooptijd van het voorafgaand onderzoek kan een knelpunt voor het samenwerkingsverband opleveren. Van Schoonhoven stelt als oplossing voor om een beroep te doen op het discretionaire karakter van de onderzoeksbevoegdheid van het Cbp. Hij overweegt daartoe dat als verwerkingen van persoonsgegevens inzichtelijk zijn gemaakt (welke gegevens gaan waar naar toe), er een privacyreglement is en een convenant van samenwerking, dit tot de gerechtvaardigde aanname kan leiden een voorafgaand onderzoek door het Cbp, gelet op de aard en strekking daarvan,

[513] Het voorafgaand onderzoek valt aan te merken als een dergelijke voorbereidingsprocedure. De Wbp gaat echter nog steeds uit van het inmiddels vervallen wettelijk stelsel. Dit betekent dat de termijnen van de procedure van het voorafgaand onderzoek zoals bedoeld in artikel 32, derde en vierde lid Wbp, op grond van de Awb inmiddels met zes weken verlengd dient te worden. Ten opzichte van het oude regime waarin bij de start van het nader onderzoek als bedoeld in artikel 32, derde lid, Wbp mededeling werd gedaan in de Staatscourant, moet onder het nieuwe regime pas mededeling plaatsvinden in de Staatscourant als er na afloop van het nader onderzoek een concept besluit is opgesteld. Tegen een dergelijk concept besluit staat evenwel voor belanghebbenden een bezwaartermijn van zes weken open.

niet opportuun te achten. De auteur meent dat het Cbp met een dergelijke overweging zou kunnen afzien van het instellen van een voorafgaand onderzoek.[514]

Ook de uitleg van strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag leidt in de praktijk tot verwarring. Het Cbp heeft de Minister van Justitie aanbevolen om artikel 31, eerste lid, onder c Wbp zo aan te passen dat de reikwijdte hiervan verhelderd wordt. Tuchtrechtelijke maatregelen zouden eveneens onder deze reikwijdte dienen te vallen nu deze gegevens moeten worden beschouwd als bijzondere gegevens in de zin van artikel 16 Wbp.[515]

6.6.2 Toezicht door de functionaris voor de gegevensbescherming

Toezicht kan ook worden uitgeoefend door de functionaris voor de gegevensbescherming. In artikel 64 van de Wbp is onder meer geregeld dat de verantwoordelijke er voor zorgdraagt dat de functionaris ter vervulling van zijn taak over bevoegdheden beschikt die gelijkwaardig zijn aan de bevoegdheden zoals geregeld in afdeling 5.2 van de Awb Uit bestudeerde literatuur en jurisprudentie blijkt niet dat deze bevoegdheden niet zijn toegekend aan functionarissen, bijvoorbeeld bij interne regeling, maar uit jaarverslagen van functionarissen kan ook niet worden afgeleid dat ze wel zijn toegekend. In het laatste geval mag verwacht worden dat daarvan in een jaarverslag melding wordt gemaakt. Zie hierover ook eerder paragraaf 6.4.3. Verder zijn er uit bestudeerde literatuur en jurisprudentie geen duidelijke knelpunten naar voren gekomen of afgeleid, anders dan dat het vorm en invulling geven van de functie een 'zoektocht' was. Zoals eerder genoemd, is er wel een actieve vereniging van functionarissen voor de gegevensbescherming, het NGFG, alsmede een actieve vereniging van functionarissen die in de overheidssector werkzaam zijn.[516]

6.6.4 Rechtsbescherming

De rechtsbescherming tegen besluiten van bestuursorganen wordt bepaald door de Awb. In de literatuur worden op dit punt geen knelpunten aan de orde gesteld. Wel worden opmerkingen gemaakt dat er een onderscheid is in de rechtsbescherming tegen besluiten van bestuursorganen en alle andere organisaties, en dat dit gedifferentieerde systeem van rechtsbescherming de privacybescherming niet ten goede komt. Tegen besluiten van bestuursorganen staat de rechtsgang van de Awb open en tegen beslissingen van alle overige organisaties dient de rechtsgang van het wetboek van Burgerlijke Rechtsvordering te worden gevolgd. Holvast benadrukt dat dit onderscheid de rechtseenheid niet bevordert. Holvast meent verder dat de rechtseenheid evenmin wordt bereikt doordat op grond van de Awb onderscheid wordt gemaakt tussen A- en B-bestuursorganen.[517]

De doorlooptijd van het voorafgaand onderzoek kan, mede vanwege de toepasselijkheid van de uniforme openbare voorbereidingsprocedure van afdeling 3.4 Awb, een knelpunt vormen, in het bijzonder voor samenwerkingsverbanden. De uitoefening van het toezicht door functionarissen voor de gegevensbescherming levert in de publieke sector nauwelijks knelpunten op. De rechtsbescherming tegen besluiten die door organisaties uit de publieke sector zijn genomen, is een andere dan die tegen besluiten die door organisaties uit de private sector zijn genomen. Dit komt volgens sommige auteurs de rechtseenheid en de privacybescherming niet ten goede.

---

[514] Van Schoonhoven 2006b, p. 60.
[515] Van Schoonhoven 2006b, p. 77-78.
[516] Zie <www.ngfg.nl>.
[517] Holvast 2004, p. 84-85; zie ook par. 4.6.2 van dit rapport.

6.7 Internationale gegevensdoorgifte

Uit de bestudeerde literatuur komen geen specifieke knelpunten ten aanzien van internationale gegevensdoorgifte in de publieke sector naar voren. Uit de in het kader van dit onderzoek gehouden bijeenkomst met domeindeskundigen bleek wel dat het Ministerie van Buitenlandse Zaken soms aanloopt tegen knelpunten, vergelijkbaar met die in de private sectior, als het gaat om de doorgifte van gegevens naar derde landen.

6.8 Uitvoeringskosten

Eén van de doelstellingen van de Wbp was om de administratieve lasten van de naleving van de meldingsplicht zo veel mogelijk te verlichten. Zoals bij het onderwerp meldingsplicht werd opgemerkt is deze doelstelling nauwelijks gerealiseerd. De uitvoeringskosten van de naleving van de meldplicht zijn hoog, althans, de uitvoeringskosten worden als gevolg van het Vrijstellingsbesluit niet beperkt. Hetzelfde geldt voor de nadere verplichtingen van de Wbp. Een verantwoordelijke die wil voldoen aan alle verplichtingen van de Wbp dient inzichtelijk te hebben welke persoonsgegevens voor welke doeleinden in zijn organisatie worden verwerkt. Daarvoor dient hij bijna dezelfde handelingen uit te voeren als die nodig zijn om aan de meldingsplicht te voldoen. Uit literatuur blijkt evenwel niet dat dit specifiek voor de publieke sector tot knelpunten aanleiding geeft.

6.9 Technologie-onafhankelijkheid

De toepassing van technologische ontwikkelingen zorgt ook binnen de publieke sector voor nieuwe discussies rond privacy en gegevensbescherming. Al genoemd zijn bijvoorbeeld de ontwikkelingen rond het Burger Service Nummer (BSN), die wordt gestuurd door de inburgering van ICT-technieken. De wens van één loket wordt steeds luider en de gescheiden overheidsregistraties, met hun impliciete privacy waarborgen, wordt in de wandelgang vaak als ouderwets bestempeld. Ook kan de ontwikkeling naar het digitaal beschikken worden genoemd. Het gaat dan om volledig geautomatiseerde beslisprocessen rond bijvoorbeeld een subsidieaanvraag die als beschikking moeten worden aangemerkt. Groothuis[518] vraagt zich daarbij af in hoeverre de praktijk daarbij in staat is de toets van artikel 42 Wbp, dat verlangt dat inzicht wordt gegeven in de logica van een geautomatiseerde individuele beslissingen, te doorstaan. Duidelijk is in ieder geval dat de Wbp nadere eisen stelt aan een dergelijke besluitvormingsproces bovenop de door het bestuursrecht geboden bescherming.

Het Cbp heeft deze ontwikkeling ook gesignaleerd en heeft er een aflevering uit de reeks 'Achtergrondstudies en Verkenningen' aan gewijd.[519] Daarmee hoopt het Cbp onder meer te kunnen bijdragen aan het richtinggeven van de ontwikkeling van de informatiehuishouding van de overheid.

6.10 Conclusies

Formeel-juridisch

Er bestaat ook in de publieke sector onduidelijkheid over de uitleg van begrippen van de Wbp. Zo blijkt het lastig te zijn te bepalen wie in de praktijk verantwoordelijk is voor het daadwerkelijk naleven van de materiële normen van de Wbp. De onduidelijkheid komt onder meer in samenwerkingsverbanden naar

[518] Groothuis 2005, p. 74.
[519] Versmissen & de Heij 2002.

voren. Ook de toepassing van deze begrippen is niet altijd werkbaar. Daarnaast is er onduidelijkheid over de verhouding van de Wbp met andere wetten, zoals de Wob en de Wet Bibob.

Naleving en handhaving

De naleving van de normatieve kaders zorgt ook voor problemen door de veelheid aan open normen. De Wbp zou daarmee te specialistisch zijn, een probleem dat ook geconstateerd werd bij de evaluatie van de voorloper van de Wbp, de Wpr. Formele zelfregulering in de vorm van gedragscodes is in de publieke sector nog niet of nauwelijks van de grond gekomen. Wel zijn er veel organisaties in de sector die zijn overgegaan tot het aanstellen van een functionaris voor de gegevensbescherming waarmee zij waarborgen willen scheppen voor een verantwoord intern toezicht. Tevens vormen verschillende publieke organisaties informele netwerken of platforms, waarbinnen zogenaamde best practices, maar ook uitwerkingen van de Wbp in concrete modellen, protocollen of andere afspraken, worden ontwikkeld. Van zelfregulering in de publieke sector is dus wel sprake, zij het op informele wijze.

Hoewel er vraagtekens te plaatsen zijn bij het realiseren van de transparantie in gegevensverwerkingen die door de Wbp wordt nagestreefd, vanwege de inhoudelijke (on)toegankelijkheid en gedetailleerdheid van het Vrijstellingsbesluit, lijkt het belangrijkste bezwaar te zijn gelegen in de administratieve lasten die naleving van de Wbp met zich meebrengt. Ondanks dat een verwerking kan zijn vrijgesteld van melding, zullen toch (bijna) dezelfde gegevens moeten worden geïnventariseerd en geregistreerd, om te kunnen voldoen aan alle verplichtingen van de Wbp. Artikel 30, derde lid Wbp is een voorbeeld van zo'n verplichting. Door sommige auteurs wordt dit artikel ook genoemd als concreet knelpunt. Wil een verantwoordelijke in staat zijn om de betrokkene te informeren over bepaalde onderdelen van een melding, dan kan de verantwoordelijke niet anders dan een registratie bijhouden van verwerkingen die zijn vrijgesteld van de meldingsplicht. Tijdens de eerder genoemde bijeenkomst met domeindeskundigen werd dit bevestigd en werd aangegeven dat een verantwoordelijke sowieso ten alle tijde zicht dient te hebben op de verwerkingen die plaatsvinden. Zou dit niet zo zijn, dan zou de verantwoordelijke niet in staat zijn de Wbp na te leven en bijvoorbeeld nooit volledig gevolg kunnen geven aan de uitoefening van rechten door betrokkenen en het nakomen van hun eigen verplichtingen.

Ten aanzien van de rechten van betrokkenen worden in de publieke sector geen belangrijke knelpunten ervaren. Wel wordt door functionarissen voor de gegevensbescherming geconstateerd dat niet altijd procedures zijn ingesteld om rechten van betrokkenen te kunnen effectueren. Uit de bestudeerde jaarverslagen en uit de bijeenkomst met domeindeskundigen komt naar voren dat, met enkele uitzonderingen, betrokkenen in het algemeen niet veel gebruik maken van hun inzage- en correctierecht. In die uitzonderingsgevallen werd het kennisnemingsrecht niet zozeer gebruikt in het kader van privacybescherming, maar voor andere doeleinden, zoals het verkrijgen van een verblijfsvergunning.

Bij het thema rechtsbescherming, handhaving en toezicht zijn enkele knelpunten naar voren gekomen. De keuze van de wetgever voor een gedifferentieerd stelsel van rechtsbescherming blijft onderwerp van discussie. Dit zou niet ten goede komen aan de rechtseenheid en de privacybescherming. De handhaving van de Wbp spitst zich met name toe op het door het Cbp meer gericht onderzoeken alsmede de uitoefening van de onderzoeksbevoegdheid in voorafgaande onderzoeken bij samenwerkingsverbanden. De lange doorlooptijd is belemmerend. Verder wordt voorgesteld een uitbreiding van de strafbaarstelling in de Wbp op te nemen omdat vervolgacties veelal uitblijven nadat het Cbp heeft geconstateerd dat een verwerking onrechtmatig is of was. Het Cbp kan zelfstandig bevoegd worden gemaakt dergelijke strafzaken af te doen.

Bij het thema internationale doorgiften zijn geen knelpunten geïnventariseerd.

Beeldvorming en bekendheid

Zoals in hoofdstuk 4 al aan de orde is gesteld, zijn verschillende auteurs van mening dat de Wbp geen bijdrage levert aan privacybescherming, maar hooguit een zorgvuldige omgang met persoonsgegevens bevordert. Ook wordt de Wbp vooral door de structuur van meldingen en het voorafgaand onderzoek als een administratieve lastenpost gezien, waardoor alleen nog tamelijk onschuldige verwerkingen conform de Wbp plaatsvinden.

Diverse jaarverslagen van functionarissen voor de gegevensbescherming bij gemeenten en ministeries, schetsen een beeld van een bewustzijn van de Wbp dat verbetering behoeft.[520] Dit zou continu de aandacht vragen en de nodige tijd kosten van de betreffende 'interne privacytoezichthouders'. Een gebrek aan bewustzijn zou bij een aantal organisaties er ook debet aan zijn dat gedurende een jaar soms in het geheel geen adviezen worden gevraagd aan de functionaris over Wbp vraagstukken en/of in het geheel geen klachten of inzageverzoeken worden ontvangen.

[520] Jaarverslag FG Gemeente Arnhem 2005, Jaarverslag FG Gemeente Best 2005, Jaarverslag FG Inlichtingenbureau 2005, Jaarverslag FG Ministerie van VROM 2003 & 2004, Jaarverslag FG Ministerie van LNV, 2003/2004, Jaarverslag FG Ministerie van EZ 2003 en Jaarverslag FG Ministerie van VWS 2003.

Hoofdstuk 7: Semi-publieke sector

7.1 Inleiding

In dit hoofdstuk wordt een weergave gegeven van de knelpunteninventarisatie in de semi-publieke sector. Onder semi-publieke sector wordt verstaan de privaatrechtelijke rechtspersonen die volledig of in aanzienlijke mate worden gefinancierd uit publieke middelen of waarvan de financiering tot de collectieve lasten wordt gerekend, zoals instellingen in de zorg- en onderwijssector, de publieke omroepen en de verschillende uitvoeringsinstanties in de sociale zekerheid.[521] In dit hoofdstuk wordt niet beoogd een uitputtende beschrijving te geven van alles wat er met betrekking tot de Wbp speelt. Op basis van literatuur- en jurisprudentieonderzoek is een beperking aangebracht tot de meest in het oogspringende knelpunten en ontwikkelingen. Uit het onderzoek is naar voren gekomen dat de meest in het oogspringende knelpunten zich voordoen in de subsector werk en sociale zekerheid en in de subsector zorg en welzijn. Hoewel er discussie mogelijk is over keuze om de zorgsector te bespreken in het kader van de semi-publieke sector, is daar toch voor gekozen omdat er in de literatuur veelal aandacht werd besteed aan de zorgsector als geheel. Geprivatiseerde delen van de zorgsector worden daarom meegenomen in dit hoofdstuk.

In de semi-publieke sector kunnen twee ontwikkelingen worden gesignaleerd die nauw samenhangen met de geconstateerde knelpunten. Ten eerste een toenemende intensivering van de samenwerking tussen organisaties waarbij de uitwisseling van persoonsgegevens een van de belangrijkste voorwaarden voor die samenwerking vormt. Hierbij kan worden gedacht aan samenwerkingsverbanden bij de uitvoering van sociale zekerheidswetgeving en de zogenaamde ketenzorg (zie paragraaf 7.3). Ten tweede blijkt uit de literatuur dat enkele knelpunten samenhangen met technologische ontwikkelingen. Het gaat hierbij onder meer om de aanstaande invoering van het landelijk elektronisch patiëntendossier (EPD), de ontwikkeling van internetportalen in de zorg en het onderwijs en de verwerking van persoonsgegevens bij de inrichting van systemen rondom de diagnose behandelcombinaties (DBC).

De knelpunten worden behandeld aan de hand van de in hoofdstuk één onderscheiden thema's te weten: werkingssfeer en toepassing, normatieve kaders, zelfregulering, transparantie en rechten van betrokkenen, handhaving, toezicht en rechtsbescherming. Het thema internationale doorgifte wordt buiten beschouwing gelaten. In de literatuur en jurisprudentie zijn geen aanwijzingen gevonden dat zich met betrekking tot deze bepalingen problemen voordoen in de semi-publieke sector. Ten slotte wordt specifiek ingegaan op knelpunten die samenhangen met de uitvoeringskosten en de technologie-onafhankelijkheid van de Wbp.

7.2 Werkingssfeer en toepassing

De algemene constatering die volgt uit de literatuur is dat door het hoge abstractieniveau de implicaties van de privacyregelgeving voor onder meer de gezondheidspraktijk, hulpverleningsinstanties en sociale uitvoeringsorganisaties niet of nauwelijks zijn te overzien. Dit wordt wel verklaard door het sectoroverschrijdende, ook wel omnibus-, karakter van de Wbp dat gebruik maakt van veel open en vage normen.[522] Dit heeft op twee plaatsen in de Wbp zijn invloed. Ten eerste in het begrippenkader dat de werkingssfeer van de wet afbakent.[523] Ten tweede door het gebruik van open en vage normen in het normenkader dat de daadwerkelijke verwerking van persoonsgegevens reguleert en normeert.[524]

---

[521] De afbakening tussen de private, publieke en semi-publieke sector wordt in hoofdstuk 1.3.2. behandeld.
[522] Zie daarover hoofdstuk 4, par. 4.2.2 en Blok 2005b.
[523] Deze worden voor wat betreft de semi-publieke sector besproken in par. 7.2.1.
[524] Zie par. 7.3.

7.2.1 Begrippen

De kernbegrippen van de Wbp, neergelegd in artikel 1 Wbp, bepalen in belangrijke mate de reikwijdte van de wet. Aan de problemen rondom het hoge abstractieniveau van de Wbp is veel aandacht besteed in de literatuur. De knelpunten die worden geconstateerd hebben betrekking op de begrippen 'persoonsgegeven', 'verwerken', 'verantwoordelijke' en 'bewerker'.

Persoonsgegeven

Een belangrijk onderdeel in de definitie van het persoonsgegeven-begrip is de natuurlijke persoon. In de gezondheidssector leidt dit onderdeel tot de vraag in hoeverre ook gegevens betreffende overleden personen moet worden aangemerkt als persoonsgegevens.[525] In 2001 oordeelde de toenmalige Registratiekamer dat het inwilligen van een verzoek tot correctie van een inmiddels overledene niet mogelijk is, ondanks dat de Wpr wel op het betreffende dossier van toepassing was en zijn partner daartoe had verzocht.[526] Maring geeft aan dat het Universitair Medisch Centrum (UMC) Utrecht er vanuit gaat dat alle gegevens van patienten, overleden of niet, onder de werking van de Wbp en de WGBO vallen, hoewel daar volgens hemzelf ook wel het een en ander tegen in te brengen is. Maring stelt dat gegevens verzameld tijdens het leven van een persoon onder de reikwijdte van de wet vallen, ook als die persoon inmiddels is overleden.

> 'Alleen gegevens die na het overlijden zijn verkregen, bijvoorbeeld tijdens de obductie, zien niet op een natuurlijk persoon en zullen derhalve niet onder de reikwijdte van de wet vallen.'[527]

Met betrekking tot het bereik van het begrip 'persoonsgegeven' en overledenen heeft de voorzieningenrechter van de rechtbank Amsterdam overwogen dat de Wbp slechts van toepassing is op gegevens die betrekking hebben op identificeerbare natuurlijke personen die nog in leven zijn.[528] Als het gaat om het verstrekken van gegevens over overleden patiënten is niets specifieks in de Wbp opgenomen. Alleen met toestemming van de betrokkene kunnen deze gegevens aan derden worden verstrekt. Deze toestemming kan in geval van overlijden vanzelfsprekend niet meer worden gegeven en staat bovendien vrijwel nooit voorafgaand aan het overlijden op schrift. In de literatuur wordt gesteld dat de arts in zo'n situatie zelfstandig moet nagaan wat de overledene zou hebben gewild, daarbij rekening houdend met alle relevante omstandigheden van het geval.[529]

Voorts stelt Ploem vast dat er onduidelijkheid bestaat met betrekking tot het element 'identificerend' als onderdeel van het persoonsgegeven-begrip. Het gaat dan om de vraag of gecodeerde gegevens in de gezondheidszorg onder de Wbp vallen. Uit toelichting op de Richtlijn 95/46/EG, overweging 26, blijkt immers dat gekeken moet worden naar:

> 'alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde personen te identificeren.'

Dat zou ook kunnen betekenen dat identificatie mogelijk is door de hulp van een arts in te zetten en de gecodeerde gegevens dus persoonsgegevens zijn waardoor zij toch onder het bereik van de Wbp vallen.[530] Dergelijke gegevens vallen blijkens de WBGO immers ook onder het beroepsgeheim. Inmiddels is duidelijk dat ook het Cbp een ruime interpretatie aan het begrip identificerend geeft, met de algemene wer-

---

[525] Blok 2003a, p. 273-278.
[526] Registratiekamer Uitspraak 10 januari 2001, z2000-1218.
[527] Maring 2003, p. 8.
[528] Vzr. Rechtbank Amsterdam 11 december 2003, *LJN* AN9893.
[529] Nouwt 2003e, p. 10.
[530] Ploem 1999. Zie ook: Van Veen 2003, p. 259-262.

kingsproblematiek van dien.[531] De ruime interpretatie van het Cbp blijkt ook uit een advies aan de Minister van OCW. De minister meende dat de geanonimiseerde gegevens die de IB-groep aan de onderwijsinspectie zou moeten gaan verstrekken, niet (meer) identificerend zijn. Het Cbp is echter niet overtuigd van de juistheid van deze conclusie:

> 'Blijkens de voorgestelde regeling zullen weliswaar geen persoonsgebonden nummers, namen en volledige geboortedata worden verstrekt, maar de overige gegevens kunnen in onderling verband toch zodanig identificerend zijn, dat niet valt uit te sluiten dat deze in bepaalde gevallen als persoonsgegevens moeten worden aangemerkt.'[532]

In samenhang met deze ruime benadering van het element identificerend adviseert het Cbp toch in sommige gevallen de gegevens dusdanig te bewerken dat er niet meer van persoonsgegevens gesproken kan worden en de Wbp dus niet van toepassing is.[533]

De onbepaaldheid van het begrip persoonsgegeven leidt tot onduidelijkheid in de reikwijdte van de wet en heeft verschillende interpretaties in de praktijk tot gevolg.

Verwerken

Met betrekking tot het begrip verwerken wordt naast de algemene kritiek vrijwel geen sectorspecifiek commentaar geleverd. Wel was er voorafgaand aan de invoering van de Wbp veel kritiek vanuit de gezondheidszorgorganisaties. De kritiek spitste zich toe op het feit dat de verkrijging nu ook onder het begrip verwerken valt.

> 'Zij (de gezondheidsorganisaties, red.) vrezen dat daarmee een onevenredige inspanningsverplichting op verantwoordelijken in de gezondheidszorg wordt gelegd.'[534]

Verantwoordelijke en bewerker

In een bij het Cbp aanhangig gemaakte klachtenprocedure klaagde een zwangere vrouw over het feit dat het gegeven dat zij zwanger was, zonder haar uitdrukkelijke toestemming, voor direct-marketing doeleinden aan een derde was verstrekt. De zaak is exemplarisch voor de onduidelijkheid die kan ontstaan voor een betrokkene bij het aanspreken het juiste bedrijf als verantwoordelijke voor de gegevensverwerking. Het Cbp erkent het voorkomen van deze onduidelijkheden:

> 'In situaties waarin meerdere natuurlijke personen of rechtspersonen betrokken zijn bij (een keten van) gegevensverwerkingen en in verband met de aard van die betrokkenheid in aanmerking komen om als verantwoordelijke in de zin van de wet te worden aangeduid kunnen zich onduidelijkheden voordoen. Deze onduidelijkheden kunnen zich met name voordoen als de juridische zeggenschap over de verwerking onvoldoende helder is, dan wel geen regeling voorhanden is op grond waarvan een bepaalde persoon of instantie daadwerkelijk door de betrokkene kan worden aangesproken.'[535]

Van der Putt wijst op soortgelijke problemen ten aanzien van de verantwoordelijke in concernverband.[536] In dit verband betoogt Nouwt dat bij de verwerking van patiëntgegevens met betrekking tot de ketenzorg het onduidelijk is wie moet worden aangemerkt als verantwoordelijke in de zin van de Wbp. Een mogelij-

---

[531] Zie par. 4.2.1 en 4.3.1 van dit rapport.
[532] Cbp Advies aan de Minister van OCW, 7 november 2002, z2002-0964.
[533] Cbp Advies aan Ministerie van VWS, 27 juli 2004, z2004-0574. In casu ging het om de verwerking van beleidsinformatie in de jeugdzorg en daarop te baseren beleidsbeslissingen.
[534] Ploem 1999.
[535] Cbp Uitspraak 8 juni 2005, z2004-0742.
[536] Van der Putt 2003, p.31-34.

ke oplossing hiervoor is dat de gezamenlijke verwerkingspartners een gezamenlijke verantwoordelijkheid op zich nemen en het beheer van het informatiesysteem overlaten aan een bewerker in de zin van de Wbp.[537] Het Cbp wijst er echter op dat dergelijke constructies niet ten koste mogen gaan van de de rechtsbescherming van betrokkene.[538]

Uit de in het kader van deze studie gehouden bijeenkomst met domeindeskundigen wordt bevestigd dat de status van een gegevensverwerker in ketenverbanden een probleem vormt. Het is lastig om daarbinnen één verantwoordelijke aan te wijzen. Individuele deelnemers nemen die rol in het algemeen niet graag op zich vanwege de daaraan gekoppelde verplichtingen. De experts gaven aan dat dit in de praktijk in sommige gevallen zelfs tot afschuiving van die verantwoordelijkheid leidt. Meer specifiek doet zich een knelpunt voor als het gaat om de toepassing van artikel 13 Wbp. De verantwoordelijke wordt daarin opgedragen zorg te dragen voor een 'passend' beschermingsniveau. Van der Wel en Homma constateren dat er bij de uitvoering van dit voorschrift onduidelijkheid heerst over de vraag wie wat mag en wie eindverantwoordelijke is voor het bepalen van de bevoegdheden in combinatie met een gedeeltelijke uitbesteding van de werkzaamheden:

> 'Organisaties die het beheer van toegangsrechten willen verbeteren lopen ook tegen de vraag op wie eindverantwoordelijke is om vast te stellen welke medewerker van de organisatie welke gegevens mag inzien of wijzigen.'[539]

In Wbp-termen hebben we het dan over de onduidelijkheid rond het verantwoordelijke-begrip in die zin dat daaraan geen natuurlijke persoon verbonden is die zich feitelijk verantwoordelijk voelt voor de gegevensverwerking. Ook de rolverdeling tussen de verantwoordelijke en bewerker blijkt in de praktijk lastig vorm te kunnen worden gegeven.

De begrippen verantwoordelijke en bewerker leiden in de praktijk tot onduidelijkheid over de status van een gegevensverwerker. De beide begrippen zijn open en vaag gedefinieerd en zijn onvoldoende op elkaar afgestemd.

7.2.2 Aansluiting met andere wetgeving

Binnen de semi-publieke sector zijn kritische geluiden waarneembaar als het gaat om de afstemming tussen de Wbp en andere wetgeving in de sector. Dat is in het kader van het thema werkingssfeer en toepassing van belang omdat sectorspecifieke regelingen een invulling (kunnen) geven aan de open en vage normen uit de Wbp en direct van invloed zijn op de toepassing van het normatief kader van de Wbp. In de semi-publieke sector gaat het om afstemming met onder meer de Wet Geneeskundige Behandelingsovereenkomst (WGBO), de Wet Bijzonder Opneming Psychiatrische Ziekenhuizen (WBOPZ), de Wet op de Jeugdzorg (WJz), en de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (Wet SUWI). In deze wetten kan vaak een verplichting worden gevonden tot de verwerking van persoonsgegevens en dus geven de daarin opgenomen voorwaarden een nadere invulling aan bijvoorbeeld het doel waarvoor persoonsgegevens mogen worden verwerkt.

Sommige auteurs wijzen erop dat de privatiseringsslag, die de afgelopen jaren in de semi-publieke sector is gemaakt, ertoe heeft geleid dat de verhouding tussen de Wbp en overige regelgeving vertroebeld is. Met de privatisering van grote delen van de semi-publieke sector (zorgverzekeringsstelsel, reïntegratiemarkt en

---

[537] Nouwt 2004, p. 232.
[538] Zie par. 7.8 waar het oordeel van het Cbp wordt besproken waarin ze de gezamenlijke verantwoordelijkheid voor het DBC-systeem wordt afgewezen. Dit zou bij de betrokkene tot onduidelijkheid leiden met betrekking tot de vraag welke instantie als verantwoordelijke aangemerkt kan worden hetgeen nadelige gevolgen kan hebben voor de effectuering van zijn Wbp-rechten.
[539] Van der Wel & Homma 2003.

WIA) zijn gevoelige gegevens bij particuliere instanties komen te liggen. Deze ontwikkeling zou vragen om stringentere regels voor de verwerking van persoonsgegevens door die bedrijven, alsmede een scherper toezicht. Volgens Van Seumeren[540] bieden de op deze sectoren toepasselijke regelingen dat helaas niet. Sectorale regelgeving kleurt de normen uit de Wbp vaak niet nader in. Tot die conclusie komt, met betrekking tot de deelsector werk en sociale zekerheid, ook het Cbp. Zij stelt zelfs dat de privatisering tot gevolg heeft dat de wetgever gegevensverwerkingen door deze private partijen minder strikt reguleert en normeert.[541]

Van den Hoven van Genderen en Gilhuis[542] noemen de combinatie van regelingen waarmee de Gemeentelijke Sociale Diensten te maken hebben zelfs een woud van regelingen. De Wbp is daar slechts een onderdeel van, samen met de Wet SUWI en de Wet Werk en Bijstand (WWB). Een soortgelijke conclusie trekt Van Eck.[543] De combinatie van regelingen leidt tot een grotere onduidelijkheid bij bijvoorbeeld reïntegratiebedrijven over welke vormen van gegevensverwerking rechtmatig zijn en welke niet. Om redenen van het 'zekere voor het onzekere' wordt er in dergelijke situaties een uitvlucht gezocht in de toestemmingsbepaling.[544] Dit is echter naar het oordeel van het Cbp niet in alle gevallen mogelijk.[545] Tijdens een werkconferentie van het Cbp over dit onderwerp gaf het Ministerie van Sociale Zaken en Werkgelegenheid aan dat zij de juridische knelpunten rond de SUWI-regeling zouden analyseren, maar dat ze terughoudend zou zijn met wetswijzigingen. Het ministerie laat oplossingen liever over aan de sector zelf.[546]

Maar juist daarvoor wordt door sommige schrijvers gewaarschuwd. Zo stellen Van de Pol en Van Seumeren[547] dat meer marktwerking in de sociale zekerheid ongetwijfeld zal leiden tot meer concurrentie tussen verzekeraars. Wanneer de concurrentie onderling groter wordt, zullen verzekeraars onder druk komen te staan om over te gaan tot risicoselectie, in ieder geval voor bepaalde producten. Ook is gebleken dat de bij zorgverzekeraars jarenlange gevoerde praktijk vaak niet voldeed aan het normenkader van de WGBO en de Wbp.[548] Reden hiervoor is volgens Straetmans[549] dat de relevantie van privacyregelgeving in een te laat stadium in het ontwikkelingstraject wordt betrokken.

Het Cbp pleit ervoor sectorale regelgeving op dit punt aan te scherpen.[550] Het gaat dan niet zozeer om de knelpunten in de verwerking, maar om de vaagheid en openheid veroorzaakt door de combinatie van regelingen. De Wbp vereist nadere specifisering en roept daarmee dit risico in het leven. Uit de gehouden expertbijeenkomst bleek de algemene verwachting dat dit afstemmingsprobleem zich in de praktijk steeds vaker voor zal gaan doen. Sectoroverschrijdende werkzaamheden worden steeds gebruikelijker. Nadere afstemming van de verschillende wettelijke regelingen is daarvoor noodzakelijk. Daarbij werd tijdens de expertbijeenkomst opgemerkt dat opdeling van de Wbp in sectorale regelgeving niet direct een oplossing voor het probleem biedt. Juist het omnibuskarakter van de Wbp kan een bindende kracht zijn in sectoroverschrijdend optreden.

Ook kan gedacht worden aan het loskoppelen van het normenkader van de Wbp en de sectorale wetgeving. Dit werd bepleit door gezondheidszorgorganisaties voorafgaand aan de invoering van de Wbp bepleit. De gezondheidszorg zou volgens de organisaties buiten de reikwijdte van de Wbp kunnen worden

---

[540] Van Seumeren 2005.
[541] Lieon & Van Munster-Frederiks 2004, p. 110.
[542] Van den Hoven van Genderen 2003, p. 2140-2156.
[543] Van Eck 2002, p. 65-71.
[544] Lieon & Munster-Frederiks 2004.
[545] Zie par. 7.3.
[546] Cbp Advies aan de minister van SZW, 12 juni 2002, z2001-0267.
[547] Van de Pol & van Seumeren 2004.
[548] Hierbij kan worden gedacht aan het gebruik van de ontslagdiagnosecode, de zorgpas en daarmee samenhangende bijzondere vereisten van art. 16 e.v. Wbp. Zie ook: Straetmans 2004, p 47-51.
[549] Straetmans 2004, p 47-51.
[550] Zie uitgebreid paragraaf 7.3.1.

gehouden omdat de bestaande gezondheidswetgeving (onder meer de WBGO, WBOPZ en Kwaliteitswet zorginstellingen) al in voldoende mate de bescherming van de persoonlijke levenssfeer waarborgt. Er zou met de Wbp sprake zijn van overregulering. Indien evenwel een privacyregime voor de gezondheidszorg onafwendbaar was dan ging de voorkeur van de zorgaanbieders uit naar een aparte wettelijke regeling, analoog aan de WGBA.[551]

De veelheid aan sectorale regelingen in combinatie met de privatisering leidt tot een voor de praktijk ondoorgrondelijk regelstelsel. De toepassing van de Wbp wordt hierdoor belemmerd.

7.3 Normatieve kaders

In deze sectie worden de belangrijkste knelpunten en ontwikkelingen besproken die in de literatuur worden gesignaleerd in de semi-publieke sector met betrekking tot de rechtmatigheid van gegevensverwerkingen, de beperkingen en de uitzonderingsgronden daarop.

7.3.1 Werk en sociale zekerheid

Uit het literatuuronderzoek komt allereerst naar voren dat de positie van de zieke werknemer voor complicaties zorgt bij de verwerking van persoonsgegevens. Het Cbp heeft in 2004 de belangrijkste privacyregels met betrekking tot zieke werknemers in kaart gebracht. Aanleiding voor het onderzoek vormde de inspanningen van de overheid om de instroom van zieke werknemers in de WAO terug te dringen door onder meer een actiever ziekteverzuimbeleid, strengere reïntegratieverplichtingen en de verplichting voor werkgevers tot het langer doorbetalen van het loon van de zieke werknemer. Door deze maatregelen is de behoefte tot uitwisseling van informatie betreffende de zieke werknemer toegenomen. Het gaat dan om de uitwisseling tussen de arbodienst, een reïntegratiebedrijf, de bedrijfsarts, het Uitvoeringsinstituut Werknemersverzekeringen en verzuimverzekeraars. De informatie is nodig voor verschillende doeleinden die uiteenlopen van controle en begeleiding tot het uitbetalen van uitkeringen.

Het Cbp komt in het onderzoek tot de conclusie dat er sprake is van een grote hoeveelheid regelmatig veranderende wetgeving die veel open normen bevat. Daardoor is het moeilijk voor betrokken partijen om te bepalen welke privacyregels voor het gebruik van persoonsgegevens van zieke werknemers in acht moeten worden genomen. Door deze onduidelijkheid kan al snel de indruk ontstaan dat privacyregels, waaronder de Wbp, hinderlijk zijn in het reïntegratieproces.[552] Verder komt uit het onderzoek naar voren dat sommige betrokken partijen graag zoveel mogelijk informatie over de zieke werknemer ontvangen vanuit het idee dat op basis daarvan de werkzaamheden het beste uitgevoerd kunnen worden. De Wbp gaat bij de verstrekking van gegevens echter uit van het noodzakelijkheidsvereiste wat inhoudt dat niet meer gegevens mogen worden verstrekt dan noodzakelijk is voor het doel van de gegevensverwerking. Deze noodzakelijkheidafweging ligt echter bij de betreffende verantwoordelijke en dat kan in de praktijk leiden tot de situatie dat meerdere verantwoordelijken in gelijksoortige situaties tot een andere afweging komen. Dit kan de uitwisseling belemmeren. Het Cbp geeft als oplossingsrichting voor dit knelpunt het formuleren van duidelijke regels omtrent dit proces. Om daartoe een aanzet te geven heeft het Cbp een document met vuistregels opgesteld voor de verschillende betrokkenen aan de hand waarvan bepaald kan worden welke gegevens rechtmatig verwerkt kunnen worden.[553]

---

[551] Ploem 1999, p. 53.
[552] Lieon & Munster-Frederiks 2004.
[553] Cbp, De zieke werknemer en privacy, vuistregels.

In de literatuur wordt erop gewezen dat het hoge abstractieniveau van de Wbp, al dan niet in combinatie met andere regelgeving, bij betrokken instanties soms kan leiden tot de indruk dat bijvoorbeeld de reïntegratie van zieke werknemers daardoor wordt belemmerd.

Naar aanleiding van het rapport 'De zieke werknemer en privacy' heeft het Cbp in 2005 een aanvullend onderzoek gedaan naar de verwerking van persoonsgegevens bij drie reïntegratiebedrijven. Zij komt daarin tot de conclusie dat de medewerkers van deze bedrijven zich ervan bewust zijn dat er bijzondere persoonsgegevens worden verwerkt en dat sprake is van een behoorlijke en zorgvuldige omgang met persoonsgegevens, hetgeen onder andere blijkt uit een geringe hoeveelheid vragen en klachten van cliënten.[554] Uit het onderzoek komt verder een knelpunt naar voren met betrekking tot de teruglevering van gegevens aan de werkgever en de arbodienst. De Wbp, in combinatie met de Wet REA en de Arbowet, geeft het reintegratiebedrijf deze mogelijkheid, maar een uitzondering moet gemaakt worden voor de gegevens waarop een medische beroepsgeheim rust. Die gegevensverwerking kan ingevolge artikel 23 Wbp slechts met toestemming van de cliënt of op basis van een wettelijke verplichting rechtmatig plaats vinden. Dit levert evenwel een probleem op omdat het reïntegratiebedrijf zich niet kan beroepen op de toestemming aangezien er sprake is van een situatie waarin de cliënt niet in vrijheid zijn toestemming kan geven. Het Cbp heeft ter oplossing van dit probleem er bij de Minister van Sociale Zaken en Werkgelegenheid op aan gedrongen om in dergelijke gevallen te voorzien zo'n een wettelijke verplichting.[555]

In aanvulling hierop kan worden opgemerkt dat de afstemming tussen de Wbp en regelingen die specifiek zijn voor de semi-publieke sector in een enkel geval voor onduidelijkheden zorgt. Illustratief daarvoor is het besluit SUWI. In haar advies ten aanzien van het conceptbesluit tot wijziging besluit SUWI oordeelde het Cbp dat de grondslag voor de gegevensverwerking door de Uitvoeringsorganisatie Werk en Inkomen (UWI) onduidelijk blijft. De verstrekking van gegevens door reïntegratiebedrijven en arbodiensten aan publieke opdrachtgevers kan op verschillende grondslagen worden teruggevoerd. Zowel artikel 8 sub c en sub f kunnen als verwerkingsgrond worden aangemerkt. De onduidelijkheid heeft evenwel tot gevolg dat er ook onduidelijkheid bestaat ten aanzien van de rechten van betrokkene om zich te verzetten (art. 40 Wbp) tegen de verwerking van de hem betreffende gegevens. Verzet is immers slechts mogelijk onder de in artikel 8 sub e en f Wbp genoemde gronden.[556] Het Cbp heeft er bij de Minister van Sociale Zaken en Werkgelegenheid op aangedrongen de grondslag voor de gegevensverwerking duidelijk te noemen in de toelichting. Soortgelijke problematiek deed zich voor rond de verwerking van het sofinummer door Arbodiensten, dat volgens artikel 24 Wbp een specifieke wettelijke grondslag behoeft. Inmiddels is in de Arbeidsomstandigheden Wet in deze grondslag voorzien.[557]

De afstemming tussen de Wbp en regelgeving in het SUWI-domein zorgt in een enkel geval voor onduidelijkheden.

De verwerking van een sofi-nummer stond ook ter discussie in een zaak die een betrokkene had aangespannen tegen de Svb. De vermelding van het sofi-nummer en de bruto-netto specificatie van de uitkering van betrokkene op haar bankafschrift beschouwde de rechtbank echter niet in strijd met artikel 11 Wbp.[558]

Meer in zijn algemeenheid kan in het SUWI-domein worden gewezen de ontwikkeling van een intensivering van samenwerking en de wens van de overheid om uitvoeringsinstanties steeds klantvriendelijker te

---

554 Cbp, Reïntegratie van zieke werknemers en privacy. Verkennend onderzoek bij drie reïntegratiebedrijven, oktober 2005.

555 Registratiekamer Advies aan de Minister van SZW, 28 november 2000, z2000-1179. Zie ook: Registratiekamer Nader advies aan aan de Minister van SZW, 1 augustus 2001, z2001-0762; Registratiekamer Advies aan de Minister van SZW, 22 september 2000, z2000-0845.

556 Cbp Advies aan Minister SZW , 21 januari 2003, z2002-1512. Nouwt 2003b, p. 2-3.

557 Art. 24, zesde lid, Arbeidsomstandighedenwet.

558 Rechtbank Maastricht 5 december 2003, *LJN* AO0044.

laten werken. Kenmerkend daarvoor is het beleidsvoornemen om eenmalig persoonsgegevens bij de klant op te halen om deze vervolgens in het gehele SUWI-traject te kunnen gebruiken.[559] Dit levert voor uitvoeringsinstanties lastige vragen op als het gaat om de toepassing van de doelbinding in o.a. artikel 9 Wbp. De 'klantvriendelijke' benadering wordt op een aantal punten belemmerd door het normatief systeem dat is vastgelegd in de Wbp.

Uit het interview dat in het kader van dit evaluatieonderzoek is gehouden met personen uit het SUWI-domein kwam naar voren dat de Wbp daardoor als belemmerend wordt ervaren. Technisch is het bijvoorbeeld mogelijk om allerlei informatie bij de verschillende instanties op te halen en te gebruiken ter verbetering van de eigen gegevensverwerking. Dan gaat het voornamelijk om de juistheid en volledigheid van de aanwezige gegevens. In de praktijk stuit men dan echter op de doelbinding, omdat er in die situatie persoonsgegevens worden gebruikt waarvan men het onduidelijk vindt of dat verenigbaar is met het doel waarvoor de gegevens zijn verkregen. Bovendien wezen de geïnterviewden erop dat het veelvuldig uitwisselen van gegevens binnen ketensamenwerking uiteindelijk kan leiden tot onduidelijkheid over waar de informatie vandaan komt en wie er verantwoordelijk voor is.

De Wbp wordt in de praktijk als belemmerend ervaren bij de uitvoering van beleid waarin toegewerkt wordt naar een 'klantvriendelijke' overheid en waarin het de bedoeling is dat eenmalig gegevens worden gevraagd aan de burger die vervolgens kunnen worden hergebruikt in het publieke en semi-publieke domein.

7.3.2 De zorgsector

Het Cbp heeft in 2005 onderzoek gedaan naar de registratie van gegevens in de zorg.[560] Het Cbp stelt dat zij in zijn algemeenheid een redelijke tot goede indruk heeft gekregen van de manier waarop met de registraties werd omgegaan. Niettemin bleek dat bij vrijwel iedere gegevensverwerking mogelijkheden voor verbetering waren, soms zelfs noodzakelijke. Verbeterpunten waren mogelijk met betrekking tot de herleidbaarheid van de geregistreerde gegevens tot een persoon. De indruk lijkt te zijn dat de praktijk daar ruimere opvattingen over heeft dan het Cbp. Verder constateerde het Cbp dat het niet altijd eenvoudig bleek om een rechtmatige grondslag te formuleren.

In de literatuur wordt met betrekking tot de zorgsector aandacht besteed aan twee ontwikkelingen die in sommige gevallen knellen met het normatief kader van de Wbp. De eerste ontwikkeling betreft de steeds belangrijker wordende samenwerking tussen zorgaanbieders en overige organisaties die betrokken zijn bij de zorg. Ten tweede ontstaan nieuwe vraagstukken rond beveiligingsaspecten als gevolg van de toepassing van nieuwe technologische toepassingen, waarmee informatieprocessen efficiënter kunnen worden ingericht. Beide ontwikkelingen hangen nauw samen aangezien informatie en communicatietechnologie (ICT) binnen samenwerkingsverbanden 'nieuwe' mogelijkheden bieden om gegevens efficiënt met elkaar uit te wisselen. In deze paragraaf worden de in de literatuur geconstateerde knelpunten besproken die samenhangen met deze twee ontwikkelingen. Daarnaast wordt aandacht besteed aan enkele specifieke knelpunten die samenhangen met de toepassing van het normatief kader van de Wbp in de zorgsector.

Beveiliging

ICT-toepassingen kunnen in de zorg veel voordelen bieden als het gaat om kostenbesparing en kwaliteitsverbetering. In de literatuur is in dat verband veel geschreven over de ontwikkeling van het Elektronisch Patiënten Dossier (EPD).[561] Het doel van het EPD is primair gelegen in het efficiënt kunnen verwerken

[559] Zie uitgebreid: <http://www.andereoverheid.nl>.
[560] Zie voor overige bevindingen: Cbp, rapport 'Landelijke zorgregistraties', 2005.
[561] Hooghiemstra 2004, p. 208-212.

van patiëntgegevens. Bij de ontwikkeling van de systemen voor het EPD moet rekening worden gehouden met de eisen die artikel 13 Wbp stelt aan het beveiligingsniveau. Ter invulling van de norm 'passend beveiligingsniveau' wordt in de systemen gebruik gemaakt van autorisatieprotocollen, authenticatieprocedures en andere beveiligingsmaatregelen. De maatregelen dienen tevens te voldoen aan de norm voor informatiebeveiliging in de zorg (NEN 7510).[562] De Inspectie voor de Gezondheidszorg heeft onderzoek gedaan naar de implementatie van de NEN-norm. Uit dat onderzoek kwam naar voren dat eind 2003 nog niet één van de twintig onderzochte ziekenhuizen de norm had geïmplementeerd en slechts in een enkele geval was deze norm voor het ziekenhuis richtsnoer om de beveiliging vorm te geven.[563] Een ander probleem betreft de onduidelijkheid over de vraag of na implementatie van deze NEN-norm voldaan is aan het 'passend beveiligingsniveau' van artikel 13 Wbp. Het Cbp heeft daarover tot op heden geen duidelijkheid gegeven.

Uit artikel 13 Wbp volgt dat de stand van de techniek en de kosten van de tenuitvoerlegging de beoordelingscriteria zijn voor het passend beveiligingsniveau. De technologische ontwikkelingen op het gebied van de informatiebeveiliging gaan bijzonder snel. Zo is het bijvoorbeeld technisch mogelijk dat kennisnemingsrechten worden gekoppeld aan een functie die een persoon vervult binnen een zorginstelling. Ook voor elektronische inzage in gegevens waarop het toestemmingsvereiste van toepassing is, kunnen systemen anticiperen.[564] Van dit soort mogelijkheden lijkt echter nog te weinig gebruik te worden gemaakt, hetgeen leidt tot de indruk dat systemen in de zorg nog niet klaar zijn voor het EPD.[565] Onvoldoende beveiliging vergemakkelijkt het onrechtmatig koppelen van verschillende bestanden en hoewel de beveiligingstechnieken vaak wel voorhanden zijn, blijken in de praktijk de reeds in gebruik zijnde EPD's niet goed beveiligd. Aanwijzingen voor die conclusie volgen uit een onderzoek dat experts van beveiligingsbedrijven in 2005 hebben gedaan naar de beveiliging van twee ziekenhuissystemen. De experts bleken de medische gegevens te kunnen inzien van 1 miljoen patiënten ondanks het feit dat artikel 13 Wbp, een passend beveiligingsniveau voorschrijft. De resultaten van dit onderzoek doen vragen rijzen met betrekking tot de werking en handhaving van artikel 13 Wbp in de zorgsector.

Eerder heeft ook Prismant geconstateerd dat het slecht is gesteld met de beveiliging van patiëntgegevens in Nederland.[566] Dat beeld wordt ook bevestigd door Van der Wel en Homma. Het probleem hangt volgens deze auteurs samen met de onduidelijkheid rond het begrip 'verantwoordelijke'.[567] Er blijkt onvoldoende overeenstemming te bestaan over de beoordelingscriteria aan de hand waarvan kan worden vastgesteld of er sprake is van een passend beveiligingsniveau. Dat blijkt ook uit de uitspraken van het Cbp waarin het beveiligingsniveau meermalen onderwerp van discussie was. Bij de beoordeling van een online diagnoseprogramma oordeelde de toenmalige Registratiekamer dat het betreffende bedrijf tekortschoot waar het ging om de beveiliging van die gegevens en in de voorlichting aan de patiënten over deze beveiliging.[568] In deze zaak werd nadrukkelijk rekening gehouden met het feit dat het bedrijf 'gevoelige' gezondheidsgegevens van de cliënten verwerkte. Daarnaast speelt het feit dat de dienst werd aangeboden via Internet een rol. Internet is een open systeem dat extra privacyrisico's met zich meebrengt.[569] Zeker wanneer gezondheidsgegevens via internet toegankelijk worden gemaakt of uitgewisseld, wijst het Cbp erop dat extra maatregelen genomen dienen te worden ter beveiliging. Dat was ook het geval bij de beoordeling van een online afsprakensysteem van het Flevoziekenhuis dat naar het oordeel van het college onvoldoende beveiligd bleek.[570]

---

[562] NEN Normcommissie Informatiebeveiliging in de Zorg, <www.nen.nl>.
[563] IGZ, 'ICT in ziekenhuizen', augustus 2004.
[564] Van Daal 2004, p. 214.
[565] Covers, Hardam &Nouwt, *JPG* 2004, p. 132.
[566] PvG, *JPG* juni 2003.
[567] Van der Wel & Homma 2003; Lucieer 2006.
[568] Registratiekamer Uitspraak 20 juni 2001, z2000-0926.
[569] Hooghiemstra 2002b.
[570] Cbp Uitspraak 9 mei 2006, z2005-1372.

Er blijft bij het ontwikkelen van ICT-toepassingen onduidelijkheid bestaan over de vraag wanneer er sprake is van een 'passend beveiligingsniveau' in de zin van artikel 13 Wbp.

Met betrekking tot het beveiligen van gegevens wijst het Cbp op de mogelijkheden die Privacy Enhancing Technologies (PET) bieden.[571] De technieken beogen kortweg de persoonlijke levensfeer te beschermen door het elimineren of verminderen van persoonsgegevens in systemen of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens. De randvoorwaarde voor toepassing van deze technieken is dat het niet gepaard mag gaan met een verlies van functionaliteit van het systeem. Naast het Cbp beveelt ook Hooghiemstra aan PET-toepassingen in te zetten bij het tot stand brengen van een 'passend beveiligingsniveau'.[572] In de interviews die gehouden zijn in het kader van dit evaluatieonderzoek bleek dat de toepassing van PET in de praktijk op praktische bezwaren stuit. Met name wordt gewezen op de hoge kosten en de relatief grote inspanningen die nodig zijn om veranderingen in een informatiehuishouding te implementeren. Deze argumenten wegen zwaarder naarmate het gaat om instanties met grotere gegevensbestanden.[573] Bovendien wordt ook in dit verband gewezen op de onduidelijkheid die er bestaat met betrekking tot de vraag wanneer er sprake is van een passend beveiligingsniveau. Om het beoordelingskader van artikel 13 Wbp te verduidelijken heeft de toenmalige Registratiekamer reeds in 2001 een rapport opgesteld dat meer concrete aanknopingspunten biedt voor de toepassing van artikel 13 Wbp.[574]

Samenwerkingsverbanden en ketenzorg

De tweede ontwikkeling die in de literatuur is besproken betreft de toenemende samenwerking binnen de zorgsector waarbij de uitwisseling van persoonsgegevens een belangrijke voorwaarde vormt. Goderie en Steketee wijzen erop dat in de praktijk bijvoorbeeld beroepskrachten een spanning ervaren tussen de geheimhoudingsplicht en de plicht kinderen in bedreigde situaties te helpen, waarvoor uitwisselen van informatie noodzakelijk kan zijn. De beroepskrachten menen in een dergelijk geval echter dat binnen het kader van de Wbp deze uitwisseling niet mogelijk is. Volgens deze auteurs is dit beeld niet terecht en biedt de regelgeving juist wel voldoende ruimte. Artikel 16 en 21 Wbp vormen in hun ogen geen belemmering bij het verstrekken van informatie, omdat de verstrekking verenigbaar dient te zijn met de zorg van een goed hulpverlener hetgeen uitwisseling van gegevens mogelijk maakt.[575] De auteurs noemen als belangrijk knelpunt, als het gaat om de informatie-uitwisseling bij ketenzorg, dat hulpverleners teveel uitgaan van wetgeving als een vaststaand feit waarvan niet of nauwelijks afgeweken mag worden. De Wbp laat echter steeds ruimte voor een belangenafweging en dat is onvoldoende bekend bij hulpverleners. Op eenzelfde probleem wijzen Baeten en Jansen als het gaat om de aanpak van huiselijk geweld. Er zijn verschillende regionale initiatieven genomen ter verbetering van de preventie en aanpak van huiselijk geweld waarbij de samenwerking tussen instellingen uit verschillende sectoren van groot belang is. Zij constateren dat de onzekerheid over de vraag of in die samenwerking gegevens over cliënten en patiënten mogen worden uitgewisseld groot is, waardoor beroepskrachten zich in de samenwerking met anderen terughoudender opstellen dan strikt genomen noodzakelijk is. Het gevolg daarvan is dat cliënten die afhankelijk zijn van de hulp en steun van diezelfde beroepskrachten deze niet krijgen.[576] Het Cbp heeft overigens voor de belangrijkste vragen met betrekking tot het uitwisselen van informatie binnen samenwerkingsverbanden een informatieblad uitgegeven.[577]

---

[571] Cbp Uitspraak 6 juni 2005, z2005-0355.
[572] Hooghiemstra 2002a en Hooghiemstra 2002b.
[573] Hierbij moet bijvoorbeeld gedacht worden aan verandering in de informatiehuishouding van de Svb waarbij het gaat om een systeem met ongeveer 5 miljoen geregistreerden.
[574] Registratiekamer, Beveiliging van persoonsgegevens, A&V nr. 23, Den Haag 2001; zie ook: Kielman en Koelewijn 2005.
[575] Goderie & Steketee 2005.
[576] Baeten & Janssen 2002.
[577] Cbp, informatieblad, nr. 31A, mei 2005.

In de literatuur wordt gewezen op de onbekenheid van hulpveleners in samenwerkingsverbanden en ketenzorg met de interpretatieruimte van de Wbp. Deze onbekendheid heeft in sommige gevallen tot gevolg dan er door hulpverleners onterecht vanuit wordt gegaan dat bepaalde gegevensverwerkingen niet mogelijk zijn.

Van Esch wijst in dat verband op een hiaat in de verwerkingsgronden van artikel 8 Wbp. Deze verwerkingsgronden bieden in sommige gevallen onvoldoende ruimte voor gegevensuitwisseling. Zijn kritiek spitst zich toe op de verwerkingsgrond die is neergelegd in sub f van artikel 8 Wbp waarin wordt bepaald dat gegevens mogen worden verwerkt wanneer sprake is van een gerechtvaardigd belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. Dit afwegingskader is volgens Van Esch zo abstract dat een hulpverlener er vaak niet mee uit de voeten kan. Daardoor komt het ook voor dat betrokken instanties onterecht de Wbp als reden opvoeren om bepaalde gegevens niet te verstrekken. Zij zijn volgens Van Esch kennelijk niet in staat bij die botsing van belangen een juiste afweging te maken:

> 'De geïnterviewde hulpverlener beklaagde zich erover dat de hulpverleningsinstanties niet bevoegd zijn onderling persoonsgegevens uit te wisselen. Blijkbaar was hij van mening dat er eerder maatregelen zouden zijn getroffen (…) indien iemand een volledig overzicht zou hebben gehad van alle gegevens omtrent het gezin.'

In dat kader concludeert de Inspectie Jeugdzorg:

> 'Er bestaat een hardnekkig beeld bij de professionals dat de Wet bescherming persoonsgegevens een absolute belemmering vormt voor het realiseren van ketenzorg in de praktijk'[578]

Van Esch stelt verder dat het wenselijk zou zijn dat ook de belangen van een derde aan wie geen gegevens worden verstrekt, een grondslag voor gegevensuitwisseling zou moeten zijn. In bepaalde gevallen kan ook het beperkte regime van de verwerking van bijzondere gegevens belemmerend werken in de jeugdhulpverlening. Gegevensuitwisseling is toegestaan voor zover het noodzakelijk is voor een goede behandeling of verzorging van de betrokkene. Bij samenwerking in het kader van de jeugdhulpverlening is een kind echter niet in relatie tot alle gegevens altijd de betrokkene waardoor de grond voor verstrekking van die gegevens komt te ontvallen.[579] In haar oratie komt Bruning evenwel tot de conclusie dat gegevensuitwisseling tussen de verschillende participanten in de jeugdhulpverlening nauwelijks wettelijke belemmeringen kent. Met betrekking tot gegevensuitwisseling is steeds heel veel mogelijk zolang er maar telkens een noodzakelijkheidstoets wordt uitgevoerd en alleen gegevens worden doorgegeven die nodig zijn voor de uitvoering van taken met betrekking tot het kind.[580] Tot een soortgelijke conclusie komt ook Terhorst in reactie op het artikel van Van Esch.[581]

Ondanks dat de Wbp nauwelijks belemmeringen aan de (jeugd)zorg oplegt, blijkt uit de literatuur dat de praktijk de Wbp wel als belemmerend ervaart.

In de literatuur wordt daarnaast aandacht besteed aan problemen in de samenwerking van hulpverlenende instanties in de bemoeizorg. Het gaat dan om hulpverlening aan mensen in psychische of sociale nood die zelf niet willen, kunnen of durven te vragen om hulp. Er bestaat tussen hulpverleners behoefte om ook bijzondere gegevens in de zin van art 16 Wbp uit te wisselen. Wanneer een betrokkene daarvoor echter geen toestemming geeft is de verstrekking en verwerking niet mogelijk, vanwege het ontbreken van een wettelijke basis.[582] Een probleem dat zich verder voordoet bij de bemoeizorg betreft de verwerking van (bijzondere) gegevens van personen die als cliënt staan ingeschreven van de openbare geestelijke gezond-

[578] Rapport Inspectie jeugdhulpverlening en jeugdbescherming e.a. 2003.
[579] Van Esch 2005, 38.
[580] Bruning 2006.
[581] Terhorst 2006.
[582] TdB 2001.

heidszorg (OGGZ). In meldpuntoverleggen tussen de thuiszorg, maatschappelijk werk, de Brijder stichting, het centrum voor GGZ, de gemeente, de politie en woningbouwcorporaties wordt deze cliënt vervolgens besproken. Op de relatie tussen de cliënt van de OGGZ en de verschillende bij de bemoeizorg betrokken hulpverleners rust echter ook een geheimhoudingsplicht. Wanneer alle deelnemers aan het meldpuntoverleg standaard aanwezig zijn tijdens iedere bijeenkomst betekent dit dat veel deelnemers ook informatie krijgen over betrokkenen waarmee zij niets te maken hebben. Bovendien kan het voorkomen dat informatie wordt uitgewisseld die, hoewel het een betrokkene betreft waarmee zij (ook) een relatie hebben, voor de uitvoering van hun taak niet noodzakelijk is. Het Cbp heeft geconcludeerd dat deze praktijk in strijd is met de artikelen 8, 9 en 11 Wbp.[583] In de praktijk is dit een probleem dat moeilijk kan worden opgelost.

Soortgelijke problemen doen zich ook voor bij de inrichting van de informatiehuishouding voor de bureaus jeugdzorg. Daarbij moet ook rekening worden gehouden met de omstandigheid dat medewerkers binnen de jeugdzorg een zwijgplicht kunnen hebben. Het komt in de praktijk echter voor dat vertegenwoordigers van de bureaus jeugdzorg bij een intakegesprek een dubbelfunctie hebben. Dat kan, met name in situaties waarin de hulpvrager reeds bekend is bij de vertegenwoordiger, tot complicaties leiden. De betreffende medewerkers dreigen regelmatig te worden geconfronteerd met een onoplosbaar dilemma. Komen in het intakegesprek namelijk 'eigen' cliënten van de medewerker ter sprake dan heeft hij enerzijds te maken met de onverkort geldende eisen van het beroepsgeheim en anderzijds met de verwachting, mogelijk ook de neiging om kennis en informatie over de hulpvrager die al eerder is verkregen te gebruiken bij de intake.

Het Cbp suggereert als oplossing dat getracht moet worden om de intake te laten doen door medewerkers die geen dubbelfunctie hebben of dat bij de eerste intake toestemming gevraagd wordt voor deze specifieke verwerking.[584]

In de zorg- en hulpverlening waarbij zonder de instemming van de betrokkene wordt gehandeld werpt de Wbp belemmeringen op in de gegevensuitwisseling.

Medisch wetenschappelijk onderzoek

Ploem signaleert twee knelpunten met betrekking tot het gebruik van persoonsgegevens voor (medisch) wetenschappelijk onderzoek die belemmerend werken bij het gebruik van persoonsgegevens in die onderzoeken. Zij stelt allereerst vast dat er onduidelijkheid bestaat met betrekking tot de juridische status van gecodeerde gegevens. Dit knelpunt hangt samen met de reikwijdte van het begrip persoonsgegeven dat reeds in paragraaf 6.2 uitgebreid aan de orde is gekomen. Vervolgens wijst zij op de (te) centrale positie van het toestemmingsvereiste bij de verwerking van bijzondere persoonsgegevens die mogelijk belemmerend kan werken bij de verwerking van de gegevens.[585] Uit de interviews die zijn gehouden in het kader van dit onderzoek werd dit eveneens naar voren gebracht als knelpunt. Anderzijds kan de kritiek op het toestemmingsvereiste worden gerelativeerd door de uitzondering die volgt uit artikel 23 lid 2 sub c Wbp. Daarin wordt bepaald dat toestemming achterwege kan blijven wanneer het vragen van toestemming onmogelijk blijkt of een onevenredige inspanning oplevert.

Het normatieve kader rond medisch wetenschappelijk onderzoek is lastig toepasbaar in de praktijk.

[583] Cbp Advies aan Dagelijks Bestuur GGD, 4 oktober 2004, z2004-0583.
[584] Cbp Uitspraak 14 januari 2002, z2001-1575.
[585] Ploem 2004.

Bijzondere gegevens

In de literatuur en jurisprudentie komen een aantal specifieke gevallen voor waarin onrechtmatig bijzondere gegevens werden verwerkt. In een klachtprocedure vormde de verwerking van gezondheidsgegevens aanleiding voor het Cbp om direct-marketing activiteiten van een apotheker als onrechtmatig te beschouwen. Het Cbp heeft geoordeeld dat een mailing van een apotheker aan zijn klanten op basis van medicijngebruik in strijd is met artikel 9 en 21 Wbp.[586] De mailing van de apotheker aan zijn eigen klanten had betrekking op het verkrijgen van de anticonceptiepil zonder recept. De onrechtmatigheid vloeide voort uit het feit dat de apotheker geen rekening had gehouden met het feit dat het ging om bijzondere gegevens.

Dezelfde mailing werd gestuurd naar klantgegevens van andere zorgverleners, waar de apotheker uit hoofde van zijn beheerderfunctie van het register toegang toe had. Deze handelswijze beschouwt het Cbp als een misbruik van die beheerderpositie en bovendien achtte zij de mailing in strijd met artikel 16 juncto artikel 21 eerste lid onder a Wbp.[587] In een ander geval ging het om een klacht van een apotheker vanwege het verstrekken van diabetestestmateriaal. De apotheker moest deze gegevens verstrekken aan een zorgverzekeraar zodat deze op individueel niveau kon controleren of de verstrekking van hulpmiddelen doelmatig geschiedde. Dit werd door het Cbp in strijd met artikel 11 Wbp geacht. Met minder ingrijpend optreden kan volgens het Cbp hetzelfde doel worden bereikt, namelijk middels een steekproefsgewijs onderzoek op geaggregeerd niveau. Indien er na een dergelijke controle reden bestaat tot nader onderzoek in een individueel geval is dat volgens het Cbp wel gerechtvaardigd.[588]

Gevers heeft in aanvulling daarop specifiek kritiek op de normering van de verwerking van genetische gegevens (art. 16 juncto art. 21 lid 4 Wbp). Hij stelt dat de Wbp daar in feite buiten het terrein treedt van de dataprotectie. Gevers vraagt zich af of een verbod om erfelijkheidsgegevens buiten de hulpverlening te verwerken, niet veel eerder een kwestie van antidiscriminatiebeleid en sociale politiek is. Hij suggereert vervolgens dat een deze regeling niet thuis hoort in de Wbp maar eerder in de andere wetgeving zoals de Wet op de medische keuringen.[589] Het Cbp beschouwt inmiddels ook DNA-materiaal als gegevens die informatie bevatten over erfelijke eigenschappen en rekent deze gegevens om die reden tot de categorie bijzondere gegevens.[590]

Ook in andere gevallen waarin vragen rijzen over de reikwijdte van de bepalingen betreffende bijzondere gegevens kleurt het Cbp de begrippen nader in. Een voorbeeld daarvan is de vraag die bij het Ministerie van OCW rees bij de invoering van een regeling ter bekostiging van onder andere het leerwegondersteunend onderwijs. De minister wilde weten of gegevens over IQ en sociaal-emotionele problematiek onder de reikwijdte van de in artikel 21 Wbp gebruikte aanduiding 'persoonsgegevens betreffende iemands gezondheid' zou vallen. Het Cbp wijst er in haar antwoord op dat het begrip gezondheid ruim moet worden opgevat:

> ' (...) het omvat niet alleen de gegevens die in het kader van een medisch onderzoek of medische behandeling door een arts worden verwerkt, maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen. Gelet op de toelichtende stukken bij het voorstel Wbp moet er naar het oordeel van het Cbp van worden uitgegaan dat gegevens over IQ en sociaal-emotionele problematiek, in elk geval bij een groot deel van de relevante doelgroep, zijn aan te merken als persoonsgegevens over iemands gezondheid. (...) De omstandigheid dat gegevens over IQ en sociaal-emotionele proble-

[586] Cbp Uitspraak 9 mei 2003, z2002-1085.
[587] Cbp Uitspraak 9 mei 2003, z2002-1085.
[588] Cbp Uitspraak 27 februari 2003, z2002-0831.
[589] Gevers 1999, p. 66.
[590] Van de Pol 2003.

matiek gegevens over eigenschappen (persoonskenmerken) zijn, sluit geenszins uit dat het hierbij ook gaat om gegevens betreffende iemands gezondheid.'[591]

In de literatuur worden vraagtekens gesteld bij opneming van de regeling rond de verwerking van genetische gegevens buiten de hulpverlening in de Wbp. Het Cbp lijkt daarentegen geneigd om de regeling rond de verwerking van bijzondere gegevens ruim uit te leggen.

7.4 Zelfregulering

De wetgever hecht bij de toepassing van de Wbp veel waarde aan zelfregulering in de vorm van gedragscodes en de Functionaris Gegevensbescherming. In deze paragraaf wordt nagegaan welke de belangrijkste gesignaleerde knelpunten zijn met betrekking tot beide zelfreguleringsinstrumenten.

7.4.1 Gedragscodes

Binnen de semi-publieke sector zijn gedragscodes in een tweetal deelgebieden van kracht. Ten eerste de Gedragscode Verwerking Persoongegevens Financiële Instellingen, die ook van toepassing is op de gegevensverwerking door de zorgverzekeraars. Ten tweede zijn er een drietal gedragscodes voor het uitvoeren van (wetenschappelijk) onderzoek, te weten (1) Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek[592], (2) Gedragscode voor gezondheidsonderzoek 'Goed gedrag' (FMWV)[593] en (3) Gedragscode voor de verwerking van persoonsgegevens bij onderzoek en statistiek.[594] Over zelfregulering in de onderzoekssector is in de literatuur echter niet meer naar voren gekomen dan is behandeld in paragraaf 7.3.

Met betrekking tot de gedragscode die mede van toepassing is op het gebruik van persoonsgegevens door zorgverzekeraars zijn een aantal vragen gerezen.[595] Straetmans constateert bijvoorbeeld dat, ondanks dat er inmiddels een respectabele hoeveelheid regels is ontstaan, de gedragsregels nog niet compleet zijn. Nieuw opgekomen vraagstukken hebben uitvoeringsproblemen in de praktijk tot gevolg.[596] Een voorbeeld daarvan is de constatering dat verzekeraars in gezondheidsverklaringen teveel gegevens vragen. Het verbond voor verzekeraars heeft daarom een nieuw model opgesteld voor gezondheidsverklaringen. Het model bevat een maximum aan gegevens die verzekeraars mogen vragen. Het verbond heeft zijn leden geadviseerd om het model per 1 april 2004 te gaan gebruiken. Uit onderzoek van de consumentenbond is echter gebleken dat in 2005 nog geen kwart van de gezondheidsverklaringen die via de proefpersonen werden verkregen conform het nieuwe model waren.[597]

In 2006 is het Addendum bij de gedragscode voor Financiële Instellingen tot stand gekomen. Het Addendum bevat kort en goed een praktische uitwerking van materiële bepalingen van de Wbp. Zo wordt duidelijk gemaakt hoe de geheimhoudingsplicht van zorgverzekeraars vorm moet worden gegeven.[598] Verder zijn er regels opgesteld voor het opvragen van (medische) gegevens bij zorgaanbieders en zijn er voorwaarden opgenomen onder welke verzekerden, geselecteerd op basis van hun medische gegevens, aange-

[591] Cbp, Advies aan de Minister van OCW, 22 april 2003, z2003-0284.
[592] *Stcrt.* 2006, nr. 1.
[593] *Stcrt.* 2004, nr 82.
[594] *Stcrt.* 2004, nr. 36.
[595] Cbp, Onderzoek Zorgverzekeraars, 'gezondheidsgegevens en privacy', mei 2006.
[596] Straetmans 2004, p 47-51.
[597] Consumentengids juli 2005, p.56-57.
[598] Kooijman 2006, nr. 3.

schreven mogen worden voor bijvoorbeeld marketingdoeleinden. Het Addendum is goedgekeurd door het Cbp.

In het Addendum is een beperktere interpretatie gegeven van het begrip gezondheid. Het begrip gezondheid in de Wbp wordt ruim opgevat. Dat betekent dat veel gegevens waarover de zorgverzekeraar beschikt kunnen worden aangemerkt als persoonsgegevens betreffende iemands gezondheid. Niet al deze gegevens vallen echter onder de medische verantwoordelijkheid van een medisch adviseur. In de toelichting op het Addendum Zorgverzekeraars wordt opgemerkt dat de 'span of control' van de medisch adviseur onwerkbaar groot wordt als bijvoorbeeld ook declaratiegegevens onder zijn verantwoordelijkheid zouden vallen. Hierdoor zou de extra bescherming die het beheer door de medisch adviseur biedt juist verwateren.

Er is echter ook kritiek op het Addendum.[599] Allereerst wordt gewezen op de relatief lange termijn, ruim drie jaar, die het duurde voordat er een gedragscode tot stand is gebracht. De oorzaak daarvoor wordt onder meer gezocht in de moeizame samenwerking met het Cbp. Verder zou het college teveel de teksten dicteren waardoor het uiteindelijk een onduidelijk en moeizaam leesbaar document is geworden. Bovendien zou het nog teveel een duplicaat van de Wbp zijn waardoor de meerwaarde van de gedragscode deels teniet wordt gedaan. De oplossing zou gezocht kunnen worden in een beperktere rol van het Cbp bij de totstandkoming van een gedragscode.

Dit roept vragen op over de flexibiliteit van de gedragscode als zelfreguleringinstrument in de semi-publieke sector. Dat beeld lijkt ook te ontstaan in de onderwijssector. Zo ligt er bij de HBO-raad al ruim twee jaar het voornemen tot de opstelling van een gedragscode. Om onduidelijke redenen is dat er nog niet van gekomen. Mogelijk hangt het samen met de geringe belangstelling van Hbo-instellingen om gebruik te gaan maken van een gedragscode.

De gedragscode die van toepassing is op zorgverzekeraars vergroot de regeldichtheid, maar is kennelijk niet in staat adequaat te reageren op nieuwe ontwikkelingen binnen de zorgsector en geeft onvoldoende vorm aan het concept van zelfregulering.

7.4.2 Functionaris gegevensbescherming

Binnen de semi-publieke sector is in verschillende organisaties, uiteenlopend van hogescholen en universiteiten tot zorginstellingen, een FG ingesteld. In de literatuur worden met betrekking tot deze sectoren geen specifieke knelpunten gesignaleerd. Wel heeft het Cbp in 2004 kritiek geuit op de Minister van Onderwijs, Cultuur en Wetenschap bij de instelling van Commissie Toezicht van Bescherming Persoonsgegevens OCW-veld (CTBP-O).[600] Door de instelling van deze commissie wekte de minister de indruk dat er onderscheid gemaakt kon worden tussen extern en intern gegevensbeheer. De CTBP-O werd gepositioneerd als de toezichthouder op het externe gegevensverkeer terwijl de FG zou moeten functioneren als de toezichthouder op het interne gegevensverkeer.

Dit onderscheid wekt volgen het Cbp de indruk van een onjuiste interpretatie van de Wbp omdat daarin geen verschil wordt gemaakt tussen intern en extern gegevensverkeer. Daarnaast wijst het Cbp erop dat noch de FG van het ministerie van OCW noch die van de IB-Groep noch de CTBP-O toezicht kan houden op verwerkingen door andere partijen in het onderwijsveld. Partijen die niet onder het ministerie vallen, zijn zelf verantwoordelijk voor hun gegevensverwerkingen. Persoonsgegevens die door derde partijen verwerkt worden, kunnen niet zonder meer rechtmatig door de CTBP-O worden opgevraagd of ingezien. De instelling van de commissie laat zien dat er kennelijk vanuit het ministerie wel de behoefte bestond tot

[599] De kritiek werd naar voren gebracht in de interviews die zijn gehouden in de eerste fase van de evaluatie en in de expert-meeting.
[600] Cbp Uitspraak 6 februari 2004, z2004-0165.

de instelling van zo'n toezichtcommissie voor het gehele onderwijsveld maar dat de Wbp daarvoor geen wettelijke basis biedt. Het Cbp wijst erop dat de in het onderwijsveld participerende organisaties ieder hun eigen FG aan kunnen aanstellen als toezichthouder binnen de organisatie.

Binnen de semi-publieke sector zijn in de literatuur geen specifieke knelpunten geconstateerd met betrekking tot de FG. Wel lijkt er vanuit het Ministerie van OCW behoefte te bestaan aan een toezichthoudende commissie die zich specifiek richt op het gehele onderwijsveld. Het Cbp wijst erop dat de Wbp geen basis biedt voor een dergelijke commissie.

7.5 Transparantie en rechten van betrokkenen

De transparantiedoelstelling wordt in de Wbp vormgegeven via de meldingsplicht en de informatieplicht. In deze paragraaf worden de in de literatuur geconstateerde knelpunten met betrekking tot deze beide plichten behandeld.

In januari 2003 meldde het Cbp dat het aantal meldingen van gegevensverwerkingen in onder meer de zorgsector achter bleef bij de verwachtingen. Dit heeft ertoe geleid dat het Cbp instellingen heeft opgeroepen alsnog over te gaan tot het melden.[601] In mei 2003 herhaalt het Cbp haar oproep omdat een groot aantal ziekenhuizen, verzekeraars en arbodiensten hun gegevensverwerkingen nog steeds niet hebben gemeld bij het Cbp.[602] Uit de literatuur komen verder geen specifieke knelpunten in de semi-publieke sector naar voren. Er kan dan ook worden volstaan met te verwijzen naar de algemeen geconstateerde knelpunten die zijn behandeld in hoofdstuk 4.

Als het gaat om de bekendheid van de verantwoordelijke met de informatieplicht dan laat het onderzoek van TNS NIPO zien dat huisartsen veel minder goed op de hoogte zijn van de Wbp en de informatieplicht dan de andere ondervraagden in het onderzoek. Minder dan 50% is bekend met de verplichtingen rond het informeren van betrokkenen. Slechts 35% is bekend met de Wbp.[603] Onderwijsinstellingen scoren in het onderzoek aanzienlijk beter. Ruim 80% van de onderzochte instellingen is op de hoogte van de Wbp en 95% meent dat de informatieplicht van toepassing is op hun organisatie. Voor wat betreft de overige semi-publieke instellingen zijn deze cijfers niet bekend. Wel constateerde het Cbp, in een verkennend onderzoek bij drie reïntegratiebureaus, dat er op een juiste manier invulling werd gegeven aan de informatieplicht.[604]

Voorts zijn er een aantal individuele gevallen bekend, waarin semi-publieke instellingen hun informatieplicht hadden geschonden. Zo stelde het Cbp een schending van de informatieplicht door het UWV vast omdat deze niet aan een betrokkene had gemeld dat haar dossier door een extern ingehuurde arts zou worden behandeld.[605] Een gedraging van de IB-groep werd door de Nationale Ombudsman als onbehoorlijk bestempeld omdat een verzoeker om informatie noch als derde noch als gemachtigde werd aangemerkt en zodoende geen antwoord ontving op zijn verzoeken.[606]

Verder zorgen de onduidelijkheden die bestaan rond het begrip 'verantwoordelijke' binnen de verschillende ketens in de semi-publieke sector (zie paragraaf 7.2.1.) ook voor knelpunten bij de invulling van de informatieplicht. Illustratief daarvoor is de klacht over de onduidelijkheden rond de verantwoordelijkheden

---

601 Cbp, nieuwsbericht: 'Cbp roept op tot naleven meldingsplicht', 21 januari 2003; Nouwt 2003c, p. 12-13.
602 Nieuwsbericht Cbp, 13 mei 2003.
603 TNS NIPO 2006.
604 Cbp, Reïntegratie van zieke werknemers en privacy. Verkennend onderzoek bij drie reintegratiebedrijven, oktober 2005.
605 Cbp Uitspraak 4 maart 2003, z2002-0230.
606 Nationale Ombudsman, rapport 2003/348, 13 oktober 2003 <www.nationaleombudsman.nl>.

en bijbehorende informatieplichten rond de internetdienst 'Digidoor'. Digidoor is een voor de scholen in Almere ontworpen systeem waarin het onderwijskundig rapport in digitale vorm wordt opgenomen ten behoeve van de verstrekking daarvan aan het voortgezet onderwijs. Het Cbp heeft na een onderzoek de betrokken scholen aangegeven dat zij verantwoordelijke zijn in de zin van de Wbp waar het gaat om de informatieverstrekking aan Digidoor. Dat betekent tevens dat de aangesloten scholen gehouden zijn de ouders te informeren en ook de gelegenheid moeten geven om correctie uit te voeren voordat het onderwijskundig rapport via Digidoor doorgestuurd wordt aan de school in het voortgezet onderwijs.[607]

Ook de onduidelijkheid rond de verhouding tussen werkgever en instanties als de arbodienst bij de uitoefening van het verzuimbeleid, heeft tot gevolg dat het lastig is om een goede invulling te geven aan de informatieplicht die op beide partijen rust.[608]

Als gevolg van onduidelijkheid rond de verantwoordelijkheid voor de informatieplicht en de onbekendheid met deze verplichting lijkt laat de naleving in sommige gevallen te wensen over.

De rechten van de betrokkene vallen uiteen in ten eerste het inzage- en verbeterrecht en ten tweede het verzetsrecht. De potentiële kracht van het kennisnemingsrecht blijkt uit een uitspraak van de rechtbank Groningen. Op grond van het Privacyreglement Kentekenregister[609] werd het kennisnemingsrecht van de betrokkene bij de Rijksdienstwegverkeer (RDW) beperkt tot inzage in de gegevens tot één jaar in het verleden. De rechtbank oordeelde in beroep dat de bepaling uit het reglement waarop deze beperking werd gebaseerd in strijd is met artikel 12 van de richtlijn en artikel 35 Wbp. De RDW moest opnieuw een beslissing op bezwaar nemen.[610] Hoewel het kennisnemingsrecht op deze wijze uiteindelijk geëffectueerd is heeft de betrokkene twee jaar op daadwerkelijke inzage moeten wachten.

Noodzakelijke voorwaarde voor de effectuering van deze rechten is wetenschap bij de betrokkene dat zijn gegevens worden verwerkt. Dat lijkt op sommige gebieden vatbaar voor verbetering. Zo heeft het Cbp de indruk dat op het gebied van de landelijke registratie van patient- en medische gegevens de patiënt weinig weet van de registratie van zijn gegevens.[611] Voorts kan de betrokken bij een beroep op het inzage- en correctierecht oplopen tegen knelpunten als gevolg van het verantwoordelijke-begrip. Zo wordt bij transmuralisering een patiënt door een keten van hulpverleners geholpen hetgeen in het kader van de samenwerking gepaard gaat met een structurele gegevensuitwisseling tussen de hulpverleners. Het is vervolgens de vraag wie de betrokken patiënt als verantwoordelijk voor de gegevensverwerking kan aanspreken. Het Cbp wijst erop dat in dergelijke gevallen in ieder geval niet de betrokkene de dupe mag worden van de onduidelijkheid:

> 'In zodanige situatie behoort aan het begrip 'verantwoordelijke' een functionele invulling te worden gegeven. Aan de hand van in het maatschappelijk verkeer geldende maatstaven moet in dergelijke gevallen worden bezien aan welke natuurlijke persoon of rechtspersoon de betreffende verwerking moet worden toegerekend.'[612]

Verder is bij het voldoen aan een inzageverzoek, de vaststelling van de identiteit van de verzoeker van belang. De verantwoordelijke is volgens de Wbp verplicht de identiteit van de betrokkene die een inzageverzoek doet, deugdelijk vast te stellen. Zo oordeelde het Cbp dat de verantwoordelijke zorgvuldig handelt indien deze vraagt om een kopie van het legitimatiebewijs om de identiteit van de verzoeker deugdelijk

---

607 Cbp Uitspraak 27 mei 2005, z2004-1152.
608 Lieon & Munster-Frederiks 2004, p. 108.
609 Het privacyreglement kentekenregister is een uitwerking van art. 45 WVW en is afgekondigd in de *Sth*, 2000/206.
610 Rechtbank Groningen, 16 juni 2005, *LJN* AT9375.
611 Cbp, 'Onderzoek Landelijke zorgregistraties, Rapport 3', Den Haag: maart 2005, p. 5.
612 Cbp Uitspraak 8 juni 2005, z2004-0742.

vast te stellen. Het ging in casu om een verzoek tot inzage bij een handelsinformatiebureau.[613] Gezien de aard van gegevens waar het hier om gaat, acht Nouwt dezelfde eisen van toepassing op een inzageverzoek in de zorgsector.[614] Het Cbp stelt zich bij de vraag of de identiteit van de betrokkene deugdelijk is onderzocht overigens terughoudend op. Dat blijkt onder meer uit een oordeel van het Cbp over de mate waarin de verantwoordelijke, in casu het UWV, zich van de identiteit van de verzoeker tot inzage moest verwittigen.[615]

Uit het onderzoek naar de rechtspraak kwam verder een zaak naar voren waarin een vader bij de school van zijn minderjarige dochter vroeg om inzage in haar gegevens. De school weigerde dat echter met een algemeen beroep op de Wbp. De rechtbank overweegt echter dat in die gevallen artikel 1:377c BW prevaleert als lex specialis ten opzichte van de Wbp:

> 'Ingeval een ouder die informatie vraagt is de Wet Bescherming Persoonsgegevens dus niet van toepassing.'[616]

Met betrekking tot het inzageverzoek ontstaan soms ook praktische bezwaren. Dat is bijvoorbeeld het geval bij het Nationaal Archief waar enkele honderden kilometers archief zijn opgeslagen. Het geven van inzage aan een betrokkene zou in zo'n geval een onevenredige inspanning kosten.[617] Er moet in die situatie dan een arbitraire keuze gemaakt worden tussen het inzageverzoek in de zin van de Wbp en het verzoek tot raadpleging in de zin van de Archiefwet.

De vergoeding voor het kennisnemingsrecht zorgt in sommige gevallen voor problemen. Binnen de gezondheidszorg doet zich hier een knelpunt voor als het gaat om de inzage in röntgenfoto's. De hoogte van de kosten die voor een inzageverzoek in rekening mogen worden gebracht, wordt bepaald door het Wbp kostenbesluit.[618] Daarin is geen aparte regeling voor het afgeven van een kopie van een röntgenfoto opgenomen, waardoor de standaardregels van toepassing zijn. Dat betekent € 0,23 per pagina met een maximum van € 4,50 per bericht.[619] Het Cbp heeft geadviseerd in het kostenbesluit op te nemen dat ook voor röntgenfoto's een vergoeding van € 22,50 per kopie gevraagd mag worden. Dit is tot op heden niet gebeurd.

Ten slotte kan worden opgemerkt dat in de literatuur niet veel is geschreven over de toepassing van het correctierecht in de semi-publieke sector. Wel heeft de Afdeling bestuursrechtspraak in haar uitspraak in een zaak van een betrokkene tegen het UWV bepaald dat het recht op verbetering en verwijdering van persoonsgegevens ingevolge artikel 36 Wbp niet bedoeld is om gegevens - die bestaan uit indrukken, meningen en conclusies over betrokkene - te corrigeren of te verwijderen.[620] De betrokkene had daartoe verzocht omdat hij zich niet kon verenigen met deze conclusies van het UWV. De afdeling legt het correctierecht van betrokkene restrictief uit en overweegt daarnaast dat het UWV kan volstaan met het toevoegen van het schriftelijk commentaar van betrokkene. Deze restrictieve uitleg bevestigd de afdeling in een zaak die een betrokkene in een soortgelijk geval had aangespannen tegen het CWI.[621]

---

[613] Cbp Uitspraak 4 februari 2003, z2002-1511.
[614] Nouwt 2003a, p. 10-11.
[615] Cbp Uitspraak 13 mei 2004, z2004-0045.
[616] Rechtbank Utrecht 17 augustus 2005, *LJN* AU1068.
[617] Zie in dit verband ook: Rechtbank Arnhem, 10 mei 2006, *LJN* AX1994.
[618] Besluit van 13 juni 2001 tot vaststelling van de vergoeding van de kosten als bedoeld in de artikelen 39 en 40 van de Wet bescherming persoonsgegevens.
[619] In twee gevallen mag een maximale vergoeding van € 22,50 in rekening worden gebracht, te weten (1) indien het afschrift bestaat uit meer dan honderd pagina's of (2) indien het bericht bestaat uit een afschrift van een, vanwege de aard van de verwerking, moeilijk toegankelijke gegevensverwerking.
[620] ABvRS 3 maart 2004, *LJN* AO4783.
[621] ABvRS 22 februari 2006, *LJN* AV2256.

Effectuering van het kennisnemingsrecht wordt bij zowel de betrokkene als de verantwoordelijke belemmerd door een aantal praktische problemen als gevolg van het hoge abstractieniveau en te rigide normstelling als het gaat om het kostenbesluit.

7.6 Handhaving, toezicht en rechtsbescherming

Uit het literatuuronderzoek komen weinig knelpunten naar voren die specifiek betrekking hebben op de rechtsbescherming, handhaving en toezicht binnen de semi-publieke sector. Hierdoor ontstaat de indruk dat het goed geregeld is. Dat blijkt ondermeer uit de resultaten van een onderzoek dat is gedaan door de Inspectie Werk en Inkomen (IWI) naar de doelbinding en de beveiliging in de keten werk en inkomen. In 2004 en 2005 werden geen klachten ingediend door burgers over het misbruik van hun persoonsgegevens.[622] Tegelijkertijd relativeert het IWI de resultaten door erop te wijzen dat het niet automatisch betekent dat gegevensbescherming ook goed geregeld is. Het Cbp heeft overigens in het kader van haar toezichthoudende taken in 2005 een samenwerkingsconvenant gesloten met de IWI. Het Convenant heeft een vijftal doelen die erop zien een effectiever en efficiënter toezicht tot stand te brengen door kennis te delen en daar waar mogelijk gezamenlijk onderzoek te verrichten. Verder ziet de samenwerking op de afstemming van de regelinterpretatie en gezamenlijk optreden in het algemeen.[623]

Naast de toenemende samenwerking in de zorg en sociale zekerheid worden ook in het kader van de bestuurlijke handhaving, samenwerkingsverbanden opgericht. Een goed voorbeeld daarvan is het convenant 'Alijda' dat het college van burgemeester en wethouders van Rotterdam in 2003 heeft gesloten met onder meer de regiopolitie, de Belastingdienst en de FIOD-ECD. Daarnaast zijn ook het UWV, de Kamer van Koophandel betrokken bij het project. De samenwerking is onder meer gericht op de integrale, ketengerichte aanpak van malafide huiseigenaren. Dit wordt onder andere gedaan door het op een zwarte lijst registreren van huiseigenaren met betrekking tot wie een indicatie bestaat dat zij zich bezighouden met malafide praktijken. Met betrekking tot de vraag wie verantwoordelijke is in de zin van de Wbp hebben de verschillende convenantpartners afgesproken dat zij gezamenlijk verantwoordelijk zijn voor de gegevensverwerking in het samenwerkingsverband. Tevens is bepaald dat betrokkenen zich steeds tot elk van de samenwerkende organisaties kunnen wenden met betrekking tot het effectueren van rechten uit de Wbp. Ingevolge artikel 8 sub e juncto 40 Wbp heeft een betrokkene recht op een heroverweging van de rechtmatigheid van de individuele gegevensverwerking. In een uitspraak van de Afdeling bestuursrechtspraak stond de vraag centraal of een registratie op de zwarte lijst van het Alijda-project moest worden aangemerkt als een besluit in de zin van artikel 1:3 Awb.[624] De rechtbank en de Afdeling oordeelden dat de registratie van betrokkene niet kan worden aangemerkt als een besluit in de zin van de Awb. In haar noot onder deze uitspraak stelt Overkleeft-Verburg dat de verantwoordelijken en ook de rechtbank ten onrechte voorbij zijn gegaan aan het verzetsrecht ingevolge de Wbp. Het bezwaar dat betrokkene aanvankelijk maakte tegen de registratie had volgens Overkleeft-Verburg als verzet moeten worden aangemerkt. Afgezien van de relevantie voor het besluitbegrip is de casus illustratief voor de relatieve onbekendheid van het verzetsrecht.

In de rechtspraak en literatuur worden weinig knelpunten gesignaleerd die specifiek betrekking hebben op de rechtsbescherming, handhaving en toezicht binnen de semi-publieke sector. Een enkele auteur wijst erop dat de onbekendheid van het verzetsrecht uit de Wbp het gevaar in zich heeft dat de rechtsbescherming van betrokkenen wordt uitgehold.

---

[622] Het rapport is gepubliceerd door de Inspectie Werk en Inkomen op 1 maart 2006.
[623] Samernwerkingsconvenant tussen het Cbp en IWI.
[624] ABvRS 12 juli 2006, *LJN* AY3726.

Uit het literatuur- en jurisprudentieonderzoek komt verder het beeld naar voren dat het Cbp in de semi-publieke sector over het algemeen effectief toezicht houdt op de uitvoering en inconsistenties van nieuwe wetgeving met de Wbp. Illustratief daarvoor zijn onder meer de wetgevingsadviezen aan de Minister van Sociale Zaken en de Minister van Onderwijs, Cultuur en Wetenschappen. In haar advies inzake de Invoeringswet en Wet Financiering Sociale Verzekeringen wees het Cbp op de problemen die de begrippen verantwoordelijke en bewerker kunnen opleveren. In het wetsvoorstel wordt een verantwoordelijke aangewezen terwijl een polisadministratie in de zin van de Wbp meerdere verantwoordelijken zal kennen.[625]

Ook met betrekking tot de Wet Marktordening Gezondheidszorg kwam het Cbp tot de conclusie dat deze in strijd zou zijn met het bepaalde in de Wbp en dringt er met klem op aan het wetsvoorstel aan te passen overeenkomstig haar advies.[626] Een ander voorbeeld betreft het advies over het bekostigingsbesluit Wet Primair Onderwijs (WPO) waarin het Cbp concludeert dat etniciteit vervalt als criterium voor het bepalen van onderwijsachterstanden. Het college wijst er vervolgens op dat het daarmee voor scholen niet langer is toegestaan gegevens rond de etniciteit van leerlingen te registeren en zij adviseert deze informatie als zodanig op te nemen in de Nota van toelichting bij het besluit.[627] Verder oordeelde het Cbp dat ten aanzien van de WPO het Besluit Informatievoorziening in strijd was met de Wbp. In de ontwerptekst wordt volgens het college niet aangetoond waarom het noodzakelijk is dat de minister de personeelsgegevens op persoonsniveau krijgt van scholen. Ook ontbreekt er naar het oordeel van het Cbp een wettelijke grondslag voor het gebruik van het sofi-nummer.[628] Daarnaast speelt het Cbp een rol in de discussie rond de invoering van het BSN. Het Cbp heeft een aantal kritische kantekeningen geplaatst bij het voorstel Wet algemene bepalingen Burger Service Nummer (BSN) met name waar het gaat om het gebruik van het BSN in de zorg.[629]

Naast wetgevingsadviezen heeft het Cbp ook verschillende uitspraken gedaan in klachtenprocedures tegen instellingen in de semi-publieke sector. Voorbeelden daarvan zijn de gegrond verklaarde klacht over een online afsprakensysteem van het Flevoziekenhuis en de klachten over de registratie van het sofi-nummer door huisartsen. Het Flevoziekenhuis maakte gebruik van een emailsysteem waarin ook diagnose-informatie werd uitgewisseld via Internet. Het Cbp concludeerde o.a. dat het systeem onvoldoende beveiligd was.[630]

Via de landelijke huisartsenvereniging werden huisartsen opgeroepen om te stoppen met het registreren van sofi-nummers van patiënten. Het Cbp concludeerde dat deze registratie in strijd is met de Wbp en dat voorkomen moet worden dat patiëntendossiers daardoor vervuilen.[631] Het sofi-nummer blijkt in de semi-publieke sector vaker onderwerp van discussie. Het Cbp adviseerde ook negatief over een pilot-project waarin de IB-groep op aanvraag van gemeenten op basis van het sofi-nummer gegevens zou verstrekken over vroegtijdige schoolverlaters. Het college kwam tot de conclusie dat er geen wettelijke basis bestond voor de uitwisseling op basis van het sofi-nummer.[632]

Uit de gehouden expertmeeting met personen uit het SUWI-domein kwam met betrekking tot de toezichthoudende taak van het Cbp naar voren dat de uitspraken en rapportages van het Cbp soms teveel het karakter hebben van pseudowetgeving waardoor te weinig ruimte blijft voor de belangenafweging van de verantwoordelijke. Overigens geldt dit niet als specifiek knelpunt voor de semi-publieke sector. Ook in de expertmeeting werd in dit verband gesuggereerd dat een terughoudender opstelling van het Cbp gewenst

---

[625] Cbp Advies aan de Minister van SZW, 1 september 2003, z2003-0872.
[626] Cbp Advies aan Minister van VWS, 13 april 2005, z2005-0070.
[627] Cbp Advies aan Minister van OCW, 14 maart 2006, z2006-0154.
[628] Cbp Advies aan Minister van OCW, 12 november 2004, z2004-1182.
[629] Cbp Advies aan de leden van de Vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties 25 oktober 2005, z2005-1198.
[630] Cbp Uitspraak 9 mei 2006, z2005-1372. Zie ook het persbericht 11 mei 2006, z2005-1372.
[631] Cbp Uitspraak 23 februari 2006, z2006-0238.
[632] Cbp Advies aan Minister van OCW, 11 juli 2005, z2005-0502.

zou zijn. Door het college zou meer een accent gelegd kunnen worden op de advisering en minder op de het inkleuren van de belangenafweging.

De verschillende wetgevingsadviezen en uitspraken van het Cbp wekken de indruk dat het toezicht op, en de handhaving van de Wbp over het algemeen goed geregeld zijn in de semi-publieke sector. Wel wordt in dit verband gewezen op het gevaar van pseudowetgeving. Met betrekking tot de rechtsbescherming vormt de onbekendheid en de daarmee samenhangende verkeerde toepassing van het verzetsrecht het meest in het oogspringende knelpunt.

7.7 Uitvoeringskosten

In het onderzoek zijn twee knelpunten naar voren gekomen als het gaat om de uitvoeringskosten van de Wbp in de semi-publieke sector. Ten eerste werd in het interview dat is gehouden met deskundigen uit het SUWI-domein, gewezen op uitvoeringskosten die samenhangen met de informatieplicht. Deze kosten kunnen in sommige gevallen bijzonder hoog oplopen als grote hoeveelheden betrokkenen moeten worden geïnformeerd. Dat probleem speelde bijvoorbeeld bij het verstrekken van persoonsgegevens door de Sociale Verzekeringsbank (Svb) aan gemeenten in het kader van de armoedebestrijding. Bij de gemeenten bestond het vermoeden dat een deel van de 65-plussers met een onvolledige AOW-uitkering, onvoldoende gebruik maakte van de mogelijkheid om een aanvullende bijstanduitkering aan te vragen.

De gemeenten waren voornemens deze groepen actief te gaan benaderen en wilden daarvoor gebruik maken van de gegevens van de Svb. In haar advies over een circulaire van de Staatssecretaris van Sociale Zaken en Werkgelegenheid inzake de gegevenuitwisseling Svb-gemeenten, kwam het Cbp tot de conclusie dat:

> '(...) geen sprake is van gegevensverwerkingen die noodzakelijk zijn om een wettelijke verplichting na te komen waaraan een verantwoordelijke onderworpen is.'

Het gevolg van deze conclusie is dat er voor deze vorm van pro-actieve dienstverlening, die overigens door het Cbp geplaatst wordt in het kader van een goede vervulling van een publiekrechtelijke taak, een informatieplicht rust op de verantwoordelijke.[633] De Svb heeft uiteindelijk ervoor gekozen haar klanten met een brief te benaderen om toestemming te vragen voor de gegevensverstrekking hetgeen aanzienlijke uitvoeringskosten met zich mee heeft gebracht.

Ten tweede is reeds in paragraaf 7.3.2 gewezen op de relatief hoge uitvoeringskosten die gepaard gaan met het toepassen van beveiligingsmaatregelen en PET-toepassingen in informatiesystemen. Hoewel de kosten van de uitvoering één van de beoordelingscriteria vormt, is het voor de verantwoordelijke uitvoeringsinstanties in de semi-publieke sector lang niet altijd duidelijk waar precies de grens ligt. Technisch zijn verschillende maatregelen, zoals encryptie, voorhanden, maar hoge uitvoeringskosten vormen een belangrijke belemmering om dergelijke maatregelen in te voeren.

Uit de semi-publieke praktijk komen signalen dat de informatieplicht en het toestemmingsvereiste bij 'grote' uitvoeringsorganisaties zorgen voor relatief hoge uitvoeringskosten. Daarnaast vormen uitvoeringskosten een belangrijk argument bij het niet toepassen van PET-technieken en beveiligingsmaatregelen in informatiehuishoudingen.

[633] Cbp Advies aan Staatssecretaris SZW, 30 maart 2004, z2004-0058.

7.8 Technologie-onafhankelijkheid

Uit het literatuuronderzoek volgt dat de technologie onafhankelijkheid van de Wbp met name in de zorgsector te wensen overlaat. Technologische ontwikkelingen zijn in de literatuur namelijk aanleiding voor een discussie over de vraag of de Wbp nog geschikt is om de technologische vooruitgang bij te houden. Van der Wel[634] constateert van niet. Hij stelt dat de praktijk de wet niet meer volgt.

> 'Als men de grofmazigheid van de ziekenhuissystemen aanvaart terwijl er nog tal van verbeteringen mogelijk zijn, en dat is vaak het geval, dan verwijdert de praktijk zich steeds verder van de oorspronkelijke wettelijke regeling.'

Inmiddels is Nederland volgens Van der Wel aangekomen bij het punt dat de huidige wettelijke regeling van het medische beroepsgeheim niet goed meer past in het huidige geautomatiseerde tijdperk. Ook Ploem[635] geeft aan dat het medisch beroepgeheim niet tegen de technologische ontwikkelingen is opgewassen. Daar waar het beroepsgeheim tekortschiet is volgens haar een belangrijke aanvullende rol voor de Wbp weggelegd. In deze benadering neemt de betekenis van de in de Wbp neergelegde regels en normen steeds meer aan belang toe. Van Ardenne[636] constateert evenwel dat de Wbp ook niet in staat is om een adequate bescherming te kunnen bieden. Met betrekking tot het landelijk Elektronisch Patiënten Dossier (EPD) stelt zij dat de invoering hiervan naar verwachting de doelmatigheid van de zorg zal vergroten en de kwaliteit verbeteren. Ongereguleerde toepassing staat echter op gespannen voet met de rechten die voor de zorgverlening van betekenis zijn. Daarbij vormt de Wbp weliswaar een antwoord op een aantal facetten, maar deze antwoorden zijn te vaag om van een adequate bescherming van patiënten te kunnen spreken.

Een ander genoemd knelpunt in relatie tot de voortschrijdende technologische ontwikkelingen is de toepassing van RFID-technieken binnen de gezondheidszorg. Dit brengt nieuwe risico's met zich mee, die onder meer nieuwe eisen stellen aan de beveiliging van dergelijke systemen.[637] Het Electronic Commerce Platform Nederland (ECP.NL) acht de Wbp wel toereikend voor RFID, maar stelt dat de abstracte bepalingen uit de Wbp nader zullen moeten worden toegespitst en worden verhelderd bij de toepassing ervan.[638]

Soms blijken ICT toepassingen in strijd met de regels en normen uit de Wbp te zijn ontwikkeld. Dat was het geval rond de inrichting van het systeem van diagnose-behandelcombinaties (DBC). In de literatuur werden vooraf vraagtekens gezet bij het gebruik van de DBC's en de inrichting van een Trusted Third Party (TTP). De kritiek spitste zich toe op het feit dat de privacy van de betrokkenen mogelijk onvoldoende gewaarborgd zou zijn omdat het de vertrouwensfunctie van de behandelaar teveel zal doorbreken.[639] Het Cbp meent bovendien dat de verzekeraar tal van andere gebruiksmogelijkheden heeft en in dat licht is het begrip 'verenigbaar gebruik' uit artikel 9 Wbp te vaag om aan dat gebruik harde grenzen te kunnen stellen. Het Cbp komt daarom tot de conclusie dat er geen wettelijke basis is voor het verstrekken van medische persoonsgegevens aan een TTP in het kader van de uitvoering van de DBC-systematiek. Om een wettelijke basis te creëren moest een inzichtelijke onderbouwing worden geven over de noodzaak om medische gegevens aan een TTP te verstrekken.[640] Uiteindelijk is besloten dat het niet noodzakelijk is

---

634 Van der Wel 2005.
635 Ploem 2001, p. 34-44.
636 E.M. van Ardenne 2003.
637 Lowethal en Wijenbergh 2004.
638 ECP.nl, 'rapport privacyrechtelijke aspecten RFID, in opdracht van EZ in samenwerking met RFID platform Nederland, mei 2005.
639 Hees 2006, p.115-117.
640 Cbp Mededeling 26 juni 2003.

dat de TTP medische persoonsgegevens verwerkt. De oplossing wordt gevonden in de clustering van de DBC's.[641]

Het Cbp kon ook niet instemmen met de instelling van een landelijk schakelpunt (LSP) waarin alle participerende zorgaanbieders gezamenlijk verantwoordelijk zouden zijn voor de verwerking en uitwisseling van persoonsgegevens. Dit zou volgens het college een zodanige pluraliteit van verantwoordelijken opleveren dat het voor betrokkenen onduidelijk wordt welke verantwoordelijke hij in geval van problemen zou moeten aanspreken. Het gevolg daarvan is dat de rechtsbescherming van betrokkenen op grond van de Wbp gevaar loopt. Daarnaast zou het voor de ingeschakelde bewerker onduidelijk zijn waar de zeggenschap van de verschillende verantwoordelijken begint en ophoudt. Het Cbp komt uiteindelijk tot de conclusie dat het creëren van een (nieuwe) wettelijke grondslag voor een dergelijk schakelpunt het meest voor de hand ligt.[642]

In de literatuur bestaat verdeeldheid met betrekking tot de vraag in hoeverre de Wbp in zijn huidige vorm én toepassing in staat is de technologische vooruitgang te reguleren en normeren. Vooral ten aanzien van technologische ontwikkelingen binnen de gezondheidszorg worden hierbij vraagtekens gezet. De ontwikkeling en inrichting van nieuwe informatiesystemen vraagt hierdoor om een constante nadere inkleuring van het normatieve kader van de Wbp.

7.9 Conclusies

In deze paragraaf worden de beschreven knelpunten aan de hand van de drie onderscheiden invalshoeken, geanalyseerd.

Formeel-juridisch

In de semi-publieke sector levert het begrip 'persoonsgegeven' evenals in de andere onderscheiden sectoren, problemen op. De onbepaaldheid van het begrip leidt tot onduidelijkheid in de reikwijdte van de wet en heeft verschillende interpretaties in de semi-publieke sector tot gevolg. Datzelfde geldt in mindere mate voor de verhouding tussen de begrippen 'verantwoordelijke' en 'bewerker'. In de praktijk laat de open en vage formulering van de beide begrippen teveel ruimte voor de interpretatie daarvan. Dit leidt in samenwerkingsverbanden in de zorg en de sociale zekerheid tot onduidelijkheid over de vraag wie in het samenwerkingsverband de verantwoordelijke en wie de bewerker is. Deze onduidelijkheid heeft niet alleen gevolgen voor de organisaties zelf maar ook voor de betrokkene omdat het voor hem daardoor niet helder is wie hij ingeval van problemen kan aanspreken. Bovendien zijn samenwerkende organisaties in die gevallen geneigd naar elkaar te verwijzen. Verder wordt in de literatuur geconstateerd dat het hoge abstractieniveau binnen de sociale zekerheid leidt tot (onnodige) belemmeringen in het reïntegratieproces van de zieke werknemer.

In de literatuur wordt gesuggereerd dat het duidelijker formuleren van de begrippen kan bijdragen aan een oplossing van dit probleem. Dit kan bijvoorbeeld door nadere invulling van de normen uit de Wbp en door aanpassing of aanscherping van sectorale regelgeving. Uit de doelstellingenanalyse in hoofdstuk 2 blijkt dat de wetgever de invulling van de normen zoveel mogelijk wilde vormgeven via zelfregulering. Op basis van de in paragraaf 7.4 geconstateerde knelpunten kan worden geconcludeerd dat het instrument van de gedragscode in de semi-publieke sector tot nu toe onvoldoende vorm heeft gegeven aan het concept van zelfregulering.

---

[641] Nouwt 2003d, p. 2.
[642] Cbp Uitspraak 21 juli 2005, z2005-0505.

Naleving en handhaving

De onduidelijkheid rond de verantwoordelijkheid heeft ook gevolgen voor het voldoen aan de informatieverplichting die verantwoordelijken hebben. Wanneer een organisatie zichzelf niet als verantwoordelijke aanmerkt, hoeft zij ook niet te voldoen aan de informatieverplichting. Bovendien is uit het onderzoek naar voren gekomen dat er binnen de semi-publieke sector, met name bij huisartsen, een relatieve onbekendheid bestaat met deze informatieverplichting met als gevolg dat de naleving daarvan te wensen overlaat.

In zijn algemeenheid geldt dat de Wbp in combinatie met de grote hoeveelheid aan sectorale regelingen en een toenemende privatisering in de semi-publieke sector leidt tot een voor de praktijk ondoorgrondelijk regelstelsel. Een 'juiste' toepassing van de wetgeving is daarom voor de praktijk bijzonder lastig. Voor een deel zou dit probleem moeten worden ondervangen door middel van zelfregulering en het opstellen van gedragscodes. Uit de praktijk komen echter signalen dat de invoering van gedragscodes een bijzonder moeizaam proces is en in sommige gevallen zelfs een tegengesteld effect heeft. Het Addendum van de zorgverzekeraars vergroot bijvoorbeeld juist de regeldichtheid en is bovendien niet in staat adequaat te reageren op nieuwe ontwikkelingen binnen de zorgsector.

In de literatuur wordt verder vastgesteld dat er verschillende technologische ontwikkelingen gaande zijn in de zorg en sociale zekerheid. Uit de bestudeerde literatuur komen aanwijzingen dat de Wbp is zijn huidige vorm en toepassing onvoldoende in staat lijkt om de technologische vooruitgang in de sectoren adequaat te kunnen reguleren. Kenmerkend daarvoor is onder meer de discussie rond het passend beveiligingsniveau in de zorg. Ook het Cbp brengt daarin, ondanks de verschillende adviezen en rapporten, niet de gewenste duidelijkheid.

Ten slotte blijkt het een probleem te zijn om in samenwerkingsverbanden in de zorgsector altijd te voldoen aan het toestemmingsvereiste voor de verwerking van bijzondere gegevens. De Wbp werpt in gevallen waarin deze toestemming niet is verkregen belemmeringen op bij de gegevensuitwisseling.

Beeldvorming en bekendheid

Onbekendheid met de Wbp zorgt in de semi-publieke sector voor een aantal problemen. In de literatuur wordt gesignaleerd dat soms te weinig aandacht wordt besteed aan de precieze implicaties van de wet voor het te ontwikkelen beleid. Een goed voorbeeld daarvan is de ontwikkeling en inrichting van nieuwe informatiesystemen. Met de toepassing van nieuwe technieken worden grenzen verschoven. Die verschuiving noopt tot een nadere inkleuring van het normatieve kader van de Wbp. Er is op dat gebied een bepaalde ruimte gelaten voor de verantwoordelijke om nadere invulling te geven aan de open en vage begrippen van de Wbp. Die ruimte wordt echter onvoldoende ingekleurd door de verantwoordelijke. Dit blijkt uit de verschillende constateringen dat in gegevensuitwisselingen waar meerdere instellingen betrokken zijn de gegevensstromen haperen. Het gaat dan om bijvoorbeeld het stroomlijnen van de aanwijzing van één verantwoordelijke. De Wbp biedt mogelijkheden, maar deze worden door de praktijk onvoldoende benut. De praktijk laat zien dat pas van inkleuring sprake is indien een ICT-toepassing stuit op bezwaren van het Cbp.

De cumulatie van regelingen zorgt voor overlap en onduidelijkheid. De Wbp is daarvan onderdeel. Daar komt bij dat in vergelijking met andere regelingen de Wbp, vanwege haar omnibuskarakter, niet uitblinkt in duidelijkheid en helderheid. Daarnaast vergroten de op gedeelten van de semi-publieke sector toepasselijke gedragscodes de regeldichtheid. De cumulatie van regelingen en de daarmee samenhangende regeldichtheid zorgt niet alleen voor situaties waarin de Wbp wordt overtreden, maar ook voor situaties waarin onterecht wordt gesteld dat de Wbp, of privacywetgeving in het algemeen, een bepaalde verwerking verbied. Zo is gebleken dat de onbekendheid met de wet ervoor zorgt dat de Wbp ten onrechte als argument gebruikt wordt om bepaalde gegevens niet te hoeven verstrekken.

Daarmee samenhangend wordt er in de literatuur op gewezen dat er in delen van de semi-publieke sector, vooral bij hulpverleners, onvoldoende bekendheid is met de wijze waarop de normen uit de Wbp kunnen,

mogen en moeten worden toegepast. Dit leidt tot een verkeerde toepassing van de wet in de praktijk die op haar beurt weer een verkeerde beeldvorming tot gevolg heeft. Uit onderzoek van TNS NIPO[643] bleek dat huisartsen (slechts 35% van de onderzochte huisartsen) niet goed op de hoogte waren van de Wbp. Onderwijsinstellingen daarentegen waren over het algemeen goed op de hoogte van de Wbp. Van de onderzochte instellingen ging het om een ruime meerderheid (80%) en bovendien meent 95% van hen dat de informatieplicht van toepassing is op hun organisatie.

[643] TNS NIPO 2006.

Hoofdstuk 8: Resultaten en vraagarticulatie

8.1 Inleiding

In de hoofdstukken 2 en 3 zijn de doelstellingen van de gemeenschapswetgever respectievelijk de nationale wetgever aan de orde gekomen. In dit hoofdstuk leggen we de doelstellingenanalyse naast de knelpuntenanalyse van de hoofdstukken 4 t/m 7. We geven allereerst weer in hoeverre de doelstellingen van de Nationale wetgever stroken met die van de Europese wetgever (par. 8.2), en hoe de doelstellingen van de Nationale wetgever zich verhouden tot de knelpuntenanalyse (par. 8.3). Wij zullen bovendien de geconstateerde knelpunten relateren aan het juridisch perspectief, handhaving en naleving, en beeldvorming, en slotte aangeven welke vragen naar onze mening in het vervolgonderzoek in aanmerking komen voor nader empirisch onderzoek (par. 8.4).

In aanvulling op het hoofdstuk over algemene knelpunten in de Wbp (hst. 4), werden knelpuntenanalyses uitgevoerd in drie sectoren: de private sector, de publieke sector en de semi-publieke sector. Enerzijds bleek dat er een groot aantal algemene knelpunten, die voor alle sectoren gelden, met betrekking tot de Wbp is geconstateerd. Dat verklaart ook de omvang van hoofdstuk 4 ten opzichte van de sectorale hoofdstukken. Anderzijds lijkt het erop, dat de private sector het meest systematisch de bezwaren heeft gearticuleerd tegen de Wbp – wat zich niet alleen uit in bezwaren specifiek voor de private sector, maar ook in algemene bezwaren die zijn geconstateerd binnen de private sector.

De publieke sector is wat betreft de persoonlijke levenssfeer waarschijnlijk het zwaarst gereguleerd: naast de Wbp gelden er veel sectorale wetten met relevantie voor bescherming van persoonsgegevens, zoals de Wet GBA, de Wet Politieregisters etcetera. De Wet GBA en WPolr zijn wetten in de zin van artikel 3 Wbp, waardoor de werking van de Wbp expliciet is uitgesloten. Daarnaast zijn er nog tal van regelingen die bepalingen bevatten over de verwerking van persoonsgegevens, maar die niet in artikel 3 Wbp genoemd worden. De Wbp heeft daarvoor aanvullende werking. Hierdoor komen veel lastige vraagstukken, die over het algemeen reden zijn voor knelpunten, buiten het bereik van de Wbp, zodat zij ook buiten het bereik van dit rapport vallen.

Een aantal opmerkingen is op zijn plaats met betrekking tot de analyse in dit hoofdstuk. Ten eerste zij opnieuw vermeld dat het onderzoek als geheel een literatuurstudie betreft, en dat de knelpunten die in deze analyse zijn gevonden, de meningen reflecteren van de auteurs van de respectievelijke publicaties. De verwijzingen naar die publicaties zijn opgenomen in de hoofdstukken over knelpunten in 't algemeen (hoofdstuk 4) en de sectorale hoofdstukken (hoofdstukken 5 tot en met 7). Deze verwijzingen worden in dit hoofdstuk niet herhaald. De vermelding van knelpunten is bovendien losgemaakt van de mate waarin zij in de literatuur worden vermeld: een kwantificatie van de ernst van het knelpunt wordt niet gegeven. Niet alle daadwerkelijke knelpunten komen noodzakelijkerwijs in de literatuur voor. Hoewel een aanzienlijke hoeveelheid literatuur in dit onderzoek meegenomen is, hebben wij niet de pretentie volledig te zijn in de analyse van knelpunten die daadwerkelijk in de literatuur zijn beschreven.

8.2 De gemeenschapswetgever en de nationale wetgever

Hoofdoelstelling van de wetgever was implementatie van de richtlijn, en die richtlijn had als belangrijkste doelen het bevorderen van de totstandbrenging en werking van de interne markt, en het beschermen van fundamentele rechten en vrijheden, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer. Voor de Wbp gelden als doelen primair de implementatie van de richtlijn, de uitvoering van de in artikel 10 tweede lid Gw neergelegde verplichting om regels te stellen ter bescherming van de persoonlijke levenssfeer, en de uitvoering van het Verdrag inzake gegevensbescherming. De laatste twee doelen zijn opnieuw direct terug te voeren tot het bereiken van bescherming van de persoonlijke levenssfeer. Hieron-

der vatten wij in een tabel de doelstellingen van de richtlijn en de Wbp samen aan de hand van de thema's die het uitgangspunt vormden voor de (sectorale) knelpuntenanalyse, met daarnaast aandacht voor de primaire en formele doelstellingen van de Europese respectievelijk de nationale wetgever. Vervolgens spreken wij ons uit over de mate waarin de materiële doelstellingen van de nationale wetgever beantwoorden aan en een reflectie zijn van de materiële doelstellingen van de richtlijn.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
primaire/formele doelstellingen	verbeteren werking van de interne markt bereiken van een gelijkwaardig beschermingsniveau bereiken van een hoog beschermingsniveau harmonisatie	implementatie van de richtlijn invulling geven aan opdracht Grondwetgever uitvoering geven aan het Verdrag Gegevensbescherming aansluiten bij art. 8 EVRM bepalen voorwaarden rechtmatige verwerkingen voorzien in kristallisatiepunt voor concretisering van normen in sectorale wetgeving, zelfregulering en jurisprudentie

Tabel 1. Primaire/formele doelstellingen

De nationale wetgever gaat bij het bepalen van de primaire doelstellingen van de Wbp niet nader in op de primaire doelstellingen van de gemeenschapswetgever met betrekking tot de werking van de interne markt en de harmonisatie. Ook de gelijkwaardigheid van het beschermingsniveau is geen punt van nadere deliberatie door de nationale wetgever. Aan de ene kant ligt het voor de hand dat alleen de gemeenschapswetgever aandacht besteedt aan de Europese dimensie van de richtlijn en de daarin vervatte doelstellingen gerelateerd aan de werking van de interne markt en de harmonisatie van beschermingsniveaus. Bovendien kan uit de feitelijke implementatie van de richtlijn worden afgeleid dat de nationale wetgever impliciet de doelstellingen van de gemeenschapswetgever overneemt. Aan de andere kant kan hieruit een gebrek aan aandacht voor de Europese dimensie van de Wbp blijken, nu de nationale wetgever niet expliciet rekening heeft gehouden met het realiseren van een gelijkwaardig beschermingsniveau en een goede werking van de interne markt. Gezien de verschillende toepassing en interpretatie van de richtlijn en de daaruit voortvloeiende wetgeving in de verschillende lidstaten zou meer nationale aandacht voor een gelijkwaardig beschermingsniveau en een goede werking van de interne markt wenselijk kunnen zijn.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
werkingssfeer en toepassing	ruime werkingssfeer die ziet op geautomatiseerde verwerkingen, en op bestanden rekening houden met bijzondere categorieën gegevens of verwerkingen	handhaven beschermingsniveau WPR aansluiten bij begrippenkader WPR om een heldere werkingssfeer te bereiken is de Wbp van toepassing daar waar geen sectorale wet anders bepaalt waar mogelijk geen onderscheid tussen verwerkingen die al dan niet onder de richtlijn vallen bereiken van een evenwicht tussen privacybescherming en andere grondrechten

Tabel 2. Werkingssfeer en toepassing

Binnen het thema werkingssfeer en toepassing concentreert de gemeenschapswetgever zich op een ruime werkingssfeer en aandacht voor gevallen die een uitzonderingsregime behoeven. De nationale wetgever richt zich op de aansluiting van de Wbp bij de Wpr, en zodoende op de continuïteit van wetgeving, het daarmee gepaard gaande beschermingsniveau, en het apparaat dat bedoeld is om dat beschermingsniveau te bereiken. Bovendien richt de nationale wetgever zich op de inbedding van de privacybescherming in de bescherming van andere grondrechten, zodat in de bescherming van verschillende aan elkaar gerelateerde grondrechten evenwicht ontstaat.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
normatieve kaders	beschermen fundamentele vrijheden bereiken van een hoog beschermingsniveau	vaststellen van een begrippenapparaat dat bruikbaar is voor rechtsvorming en voor de afweging van belangen goede inbedding in en aansluiting bij het Nederlandse rechtsstelsel positie van betrokkenen versterken door het verantwoordelijke-begrip te verhelderen rekening houden met potentiële risico's van gegevensverwerkingen waarborgen bieden tegen verwerkingen die afbreuk doen aan de werking van andere grondrechten

Tabel 3. Normatieve kaders

In de vergelijking van doelstellingen van de gemeenschapswetgever en de nationale wetgever met betrekking tot de normatieve kaders valt met name op dat de doelstellingen zoals geformuleerd door de nationale wetgever concreter zijn, en kunnen worden beschouwd als een nadere invulling van de beschermingsdoelstellingen van de gemeenschapswetgever. Daarbij is onder meer aandacht voor de bruikbaarheid van het begrippenapparaat dat voor de Nederlandse wet wordt gebruikt, de inbedding in het Nederlandse rechtsstelsel, en het stellen van waarborgen voor de bescherming van de werking van andere grondrechten.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
zelfregulering	bevordering van opstelling gedragscodes om in te spelen op behoeften en omstandigheden van een sector of branche	nadere invulling, in verband met de verwerkingscontext, van materiële normen via zelfregulering bevorderen opstelling gedragscodes door inspraakmogelijkheden te schrappen invullen eigen verantwoordelijkheid van verantwoordelijken door instelling van FG inspelen op eigen specifieke behoeften door het instellen van de meldingsplicht

Tabel 4. Zelfregulering

De doelstellingen van de nationale wetgever met betrekking tot het thema zelfregulering zijn opnieuw een nadere invulling van de doelstelling van de gemeenschapswetgever. Daarbij is onder meer aandacht voor verwerkingscontext die ook door de gemeenschapswetgever onderscheiden wordt, de invloed die deze context moet hebben op de invulling in nadere normen in gedragscodes, en het instituut van de 'functionaris gegevensbescherming', die een rol heeft in het invullen van de eigen verantwoordelijkheid van instellingen en bedrijven bij de vormgeving en handhaving van regels voor de verwerking van persoonsgegevens.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
transparantie en rechten van betrokkenen	vergroten van de transparantie van gegevensverwerkingen door toekenning van rechten en plichten aan betrokkenen en verantwoordelijken	vergroten van de transparantie van gegevensverwerkingen door toekenning van rechten en plichten aan betrokkenen en verantwoordelijken verbeteren van de positie van betrokkenen

Tabel 5. Transparantie en rechten van betrokkenen

Met betrekking tot het thema 'transparantie en rechten van betrokkenen' zijn de doelstellingen van de gemeenschapswetgever en de nationale wetgever vergelijkbaar. Vanzelfsprekend zijn in verband daarmee door de nationale wetgever specifieke rechten en plichten voorzien, zoals de meldingsplicht en het kennisnemingsrecht. Doel van de wetgever is daarmee de positie van betrokkenen te verbeteren ten opzichte van hun positie onder de Wpr.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
toezicht en rechtsbescherming	naleving van de privacyregels door instelling van een onafhankelijke toezichthouder naleving van de privacyregels door toegang tot de rechter te bieden naleving van de privacyregels door instelling van passende sancties	verbreden maatschappelijk draagvlak Cbp door toekenning bevoegdheden, en rechterlijke toetsing daarvan waarborgen onafhankelijkheid door het Cbp de status van zelfstandig bestuursorgaan te geven voorkomen belangenverstrengeling bij de toezichthouder door toetsing Cbp-bestuursreglement effectieve handhaving door het Cbp door bestuursdwang en bestuurlijke boetes laten aansluiten van de rechtsbescherming van betrokkenen bij het algemene recht versterken van de positie van verantwoordelijken t.o.v. het Cbp ophelderen positie verantwoordelijken t.o.v. Cbp door opstelling bestuursrechtelijke rechtsgang

Tabel 6. Toezicht en rechtsbescherming

De doelstellingen met betrekking tot toezicht en rechtsbescherming van de gemeenschapswetgever concentreren zich op de instelling van een onafhankelijke toezichthouder, het bieden van een rechtsingang, en het afdwingen van naleving met passende sancties. De nationale wetgever concentreert zich op het creëren van randvoorwaarden voor het functioneren van de Nederlandse toezichthouder: het College bescherming persoonsgegevens. Daarbij wordt eveneens invulling gegeven aan met name de bestuursrechtelijke handhaving, en het creëren van een evenwichtig tussen de actoren, met name tussen verantwoordelijken en het Cbp.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
internationale gegevensdoorgifte	geen onnodige belemmering van het internationale handelsverkeer, terwijl tegelijkertijd geen afbreuk wordt gedaan aan het gelijkwaardige en hoge beschermingsniveau	instrumentarium waarmee zonder belemmering van het handelsverkeer wordt voorkomen dat de wet wordt omzeild of ontdoken bij ontbreken van beroep op de uitzonderingen op het doorgifteverbod is bij wijze van 'noodklep' het instrument van een doorgiftevergunning

Tabel 7. Internationale gegevensdoorgifte

De doelstellingen van de gemeenschapswetgever en de nationale wetgever liggen met betrekking tot het thema 'internationale gegevensdoorgifte' in elkaars verlengde: het verschaffen van een instrumentarium dat aan de ene kant onnodige belemmeringen van het internationale handelsverkeer voorkomt, en aan de andere kant erop ziet dat het beschermingsniveau hoog blijkt. De nationale wetgever voorziet bij wijze van uitweg of 'noodvoorziening' in een doorgiftevergunningenstelsel.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
uitvoeringskosten	vermindering administratieve lasten	ruim gebruik van vrijstellingen op de meldingsplicht eenvoudige melding daar waar deze wel vereist is verminderen kosten door mogelijk maken melding bij functionaris gegevensbescherming

Tabel 8. Uitvoeringskosten

De doelstelling van vermindering van administratieve lasten zijn door de nationale wetgever nader ingevuld aan de hand van figuren uit de Wbp, zoals vrijstellingen op de meldingsplicht, eenvoudige melding, en melding bij de functionaris gegevensbescherming.

Type doelstelling	Doelstellingen gemeenschapswetgever	Doelstellingen nationale wetgever
technologie-onafhankelijkheid	opstellen van toekomstbestendige en niet gemakkelijk te ontduiken regelgeving	bereiken technologie-onafhankelijkheid van de regelgeving evenwicht tussen duidelijke regels en technologie-onafhankelijke regelgeving

Tabel 9. Technologie-onafhankelijkheid

Voor wat betreft het thema 'technologie-onafhankelijkheid' beperkt de gemeenschapswetgever zich tot het voorkomen van ontduiking of omzeiling van de regelgeving doordat gebruik wordt gemaakt van technologie die ten tijde van de totstandkoming van de richtlijn niet was voorzien. De nationale wetgever vult die toekomstbestendigheid nader in door op technologie-onafhankelijkheid aan te sturen, waarbij evenwicht tussen die technologie-onafhankelijkheid en de duidelijkheid van regels aanwezig moet zijn.

8.3 Verwezenlijking doelstellingen

De knelpunten geconstateerd in de literatuur over de Wbp zijn in de voorgaande hoofdstukken zijn steeds gerelateerd aan de thema's die in de wet zelf worden behandeld: werkingssfeer en toepassing, normatieve kaders, zelfregulering, transparantie en rechten van betrokkenen, toezicht en rechtsbescherming, en internationale gegevensdoorgifte; en aan twee aanvullende thema's uit de parlementiare geschiedenis: uitvoeringskosten en technologie-onafhankelijkheid. In deze paragraaf leggen wij de 'grootste gemene deler' van deze knelpuntenanalyses naast de doelstellingen van de Wet. Voor elk van thema's geven wij eerst een kort overzicht van centrale doelstellingen en knelpunten. Indien een knelpunt rechtstreeks betrekking heeft op een doelstelling, dan wordt het knelpunt bij de doelstelling vermeld. Indien dat niet het geval is, maar het knelpunt wel op het thema betrekking heeft, wordt het in het onderste gedeelte van de tabel vermeld.

Vervolgens bespreken we aan de hand van de tabellen de mate waarin aan de hand van de literatuur kan worden gesteld dat de wetgever erin geslaagd is de doelstellingen van de Wbp te verwezenlijken. Daarbij zij aangemerkt, dat de knelpunten gebaseerd zijn op constateringen in de literatuur. De mate waarin het knelpunt in de praktijk daadwerkelijk een probleem vormt, laat zich daarmee zelden of niet geven. Knelpunten zullen in ernst variëren. Wij hebben er bewust voor gekozen in de tabellen geen prioritering tussen knelpunten aan te brengen. Daarentegen worden zowel in de toelichting op de tabel en met name in de vraagarticulatie de naar onze mening belangrijkste knelpunten vermeld.

Ten slotte zij opgemerkt dat wij hieronder voorbijgaan aan de mate waarin de formele doelstellingen van de nationale wetgever zijn gerealiseerd: deze hebben alle te maken met het implementeren van of aansluiten bij rechts- of verdragsregels. Een uitzondering hierop vormen de bepaling van voorwaarden voor rechtmatige verwerking en het voorzien in kristallisatiepunten voor concretisering van normen. Deze zullen echter als onderdeel van de materiële doelstellingen hieronder aan de orde komen.

8.3.1 Werkingssfeer en toepassing

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
handhaven beschermingsniveau WPR		
aansluiten bij begrippenkader WPR		
de Wbp is van toepassing daar waar geen sectorale wet anders bepaalt	de veelheid aan sectorale regelingen in combinatie met de privatisering leidt tot een voor de praktijk ondoorgrondelijk regelstelsel; de toepassing van de Wbp wordt hierdoor belemmerd	semi-publiek
geen onderscheid tussen verwerkingen die al dan niet onder de richtlijn vallen		
bereiken van een evenwicht tussen privacybescherming en andere grondrechten	gedeeltelijke niet-toepassing van de wet op verwerkingen met journalistieke, artistieke en literaire doeleinden leidt tot vragen over de rechtsbescherming en handhaving van de bepalingen die wel van toepassing zijn, en de toepasselijkheid op nieuwe 'media', zoals weblogs	algemeen
	ingewikkeldheid en inflexibiliteit als gevolg van het algemene, omnibuskarakter van de wet	algemeen

Knelpunten buiten doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
	onduidelijkheid en onbepaaldheid van de wettelijke begrippen; deze kan onder meer technologische ontwikkeling en innovatie belemmeren, en in de weg staan aan naleving van de wet	algemeen
	verwerkingen van vestigingen van een verantwoordelijke in meerdere lid-staten zijn onderworpen aan verschillende nationale regimes	algemeen
	de toepasselijkheid van de Wbp is niet noodzakelijkerwijs gerelateerd aan de mate waarin de verwerking verband houdt met Nederland	algemeen
	de begrippen verantwoordelijke en bewerker leiden in de praktijk tot onduidelijkheid over de status van een gegevensverwerker; beide begrippen zijn open en vaag gedefinieerd en zijn slecht op elkaar afgestemd	algemeen
	de begrippenapparaten uit diverse wetten (bijv. Wbp versus Databankenwet, Aanpassingswet richtlijn inzake elektronische handel, Wet openbaar van bestuur) sluiten niet altijd op elkaar aan, wat tot interpretatiemoeilijkheden en bevoegdheidsconflicten bij toezichthouders kan leiden	algemeen
	de Wbp heeft beperkte waarde als regulerend instrument voor gegevensverwerkingen op het internet, waaronder websites en e-mail	algemeen
	de Wbp laat zich lastig toepassen in internationale verhoudingen, mede door de interpretatie van het begrip 'vestiging', en door de technische inrichting van websites, die zich over meerdere jurisdicties kan uitstrekken	algemeen
	niet alleen óf, maar hóe en in welke combinatie persoonsgegevens verwerkt worden, is van belang voor de vraag of die verwerkingen legitiem zijn; de Wbp ziet niet op deze combinaties	algemeen
	de procedurele vereisten van de Wbp leiden niet automatisch tot materiële bescherming van persoonlijke/informationele levenssfeer van betrokkenen	algemeen
	het verbod op verwerking van bijzondere gegevens kan (in letterlijke termen van de Wbp) niet doorbroken worden door een vitaal belang van betrokkene; hoewel algemene beginselen dat verbod kunnen doorbreken	algemeen
	de toepasselijkheid van de Wbp in internationale verhoudingen en bij gegevensstromen binnen een groep van ondernemingen is onduidelijk	privaat
	de toepasselijkheid van de Wbp bij internationale gegevensstromen is onduidelijk	privaat
	de onbepaaldheid van het begrip persoonsgegeven leidt tot onduidelijkheid in de reikwijdte van de wet en heeft verschillende interpretaties in de praktijk tot gevolg	semi-publiek

Tabel 10. Knelpunten werkingssfeer en toepassing

Uit de tabel hierboven kan worden afgelezen dat de meeste knelpunten met betrekking tot werkingssfeer en toepassing buiten het bereik vallen van de expliciete doelstellingen van de nationale wetgever. Omdat deze laatste nadruk heeft gelegd op de aansluiting van de Wbp bij de WPR, lijken de vele geconstateerde knelpunten in de begripsreikwijdte en –toepassing van de Wbp mogelijk ten dele terug te voeren op de gewenste aansluiting bij de WPR. Bovendien voorziet de Wbp in een gelaagd stelsel van regelgeving, zodat de gevraagde concretisering van begrippen eigenlijk te vinden zouden moeten zijn in lagere regelgeving en in zelfregulering.

De Wbp is een algemene wet voor wat betreft de toepassingsbreedte, die sectoroverschrijdend is. Met betrekking tot de werkingssfeer zijn schijnbaar tegengestelde knelpunten gevonden: onbepaaldheid van het

reguleringsinstrumentarium tegenover een te grote specificiteit daarvan. De toepassing van algemene en technologie-onafhankelijk bedoelde begrippen ('persoonsgegevens', 'verantwoordelijke', 'bewerker') in de Wbp maakt de toepassing van deze wet lastig. Hoewel het begrippenapparaat niet in *termen* van technologie is gedefinieerd, sluit het instrumentarium wel degelijk aan bij een nog vergaand gecentraliseerd begrip van gegevensverwerking dat eigen is aan de stand van de automatisering tot in de jaren negentig. Daarbij werd geen rekening gehouden, en *kon* wellicht ook geen rekening worden gehouden, met bijvoorbeeld decentralisatieverschijnselen die eigen zijn aan het gebruik van internet (Lindqvist-arrest). Daarnaast houdt de Wbp niet wezenlijk rekening met nieuwe technologie, zoals RFID, die een ander type gegevens en een ander type gegevensverwerking impliceert.

De doelstellingen van de nationale wetgever op het gebied van werkingssfeer en toepassing hebben betrekking op de aansluiting bij de WPR, de voorrang van sectorale wetgeving op de Wbp, een gelijk regime voor alle verwerkingen, en evenwicht tussen privacybescherming en andere grondrechten. Naar aanleiding van de in kaart gebrachte knelpunten constateren wij dat (a) de aansluiting bij de WPR wel in enige maar toch niet een significant onderwerp van discussie in de literatuur is geweest, (b) het begrippenapparaat van de Wbp moeilijk hanteerbaar blijkt in de praktijk, zowel door het gebruik van open begrippen als door de aansluiting tussen Wbp en andere wetgeving, en (c) de wet de nadruk legt op verwerkingen in het algemeen, terwijl het *karakter* of de *risico's* van de verwerking wellicht nadere aandacht behoeft.

8.3.2 Normatieve kaders

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
vaststellen van een begrippenapparaat dat bruikbaar is voor rechtsvorming en voor de afweging van belangen	de Wbp is eenzijdig procedureel gericht, met weinig harde materiële normen	algemeen
	de Wbp is onpraktisch, omdat deze ervan uitgaat dat élke verwerking aan de normen van de Wbp getoetst wordt, en omdat die normen te vaag zijn	algemeen
	het doelbindingsbeginsel heeft beperkte betekenis omdat het te vrijblijvend is geformuleerd	algemeen
	de gevoeligheid van bijzondere gegevens is afhankelijk van de context waarin zij worden verwerkt; het regime voor bijzondere gegevens doet aan deze diversiteit geen recht	algemeen
	het antwoord op de vraag hoe toestemming van minderjarigen kan worden verkregen, is onbepaald	algemeen
	de begrippen 'toestemming' en 'gerechtvaardigd belang' zijn lastig bepaalbaar voor de verantwoordelijke	privaat
	de normatieve kaders van de Wbp zijn soms heel specifiek en strikt, soms heel abstract	privaat
	de rol van de verantwoordelijke in de interpretatie en toepassing van het normatieve kader van de Wbp leidt tot problemen bij begrippen als 'toestemming' en 'gerechtvaardigd belang'	privaat
	het abstractieniveau van de normatieve kaders zorgt voor (onnodige) belemmeringen in het reïntegratieproces van de zieke werknemer; het door de wet geboden instrumentarium voldoet niet aan de vereisten die in de sector worden gesteld	semi-publiek
goede inbedding in en aansluiting bij het Nederlandse rechtsstelsel	er worden problemen ervaren bij de aansluiting tussen Wbp en sectorale wetten, en bij de toepassing van deze algemene wet op gevallen in specifieke sectoren	algemeen
positie van betrokkenen versterken door het verantwoordelijke-begrip te verhelderen	de interpretatie van wie heeft te gelden als verantwoordelijke levert problemen op, die rechtstreeks doorwerken in de gelding van materiële normen ten aanzien van de verantwoordelijke	algemeen

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
rekening houden met potentiële risico's van gegevensverwerkingen	de toestemmingsvarianten in de richtlijn en de wet kunnen met name in een online-omgeving tot knelpunten leiden	algemeen
	onrechtmatige toegang tot (bijzondere) gegevens door derden	privaat
	de Wbp is niet in staat een 'passend beveiligingsniveau' in de zorg af te dwingen	semi-publiek
waarborgen bieden tegen verwerkingen die afbreuk doen aan de werking van andere grondrechten		
Knelpunten buiten doelstellingen nationale wetgever	**In literatuur geconstateerde knelpunten**	**Relevante sectoren**
	het verbod van verwerking van bijzondere persoonsgegevens levert conflicten op met andere wetgeving	publiek
	het verwerken van persoonsgegevens in samenwerkingsverbanden kan problemen opleveren	publiek
	in de zorg- en hulpverlening waarbij zonder de instemming van de betrokkene wordt gehandeld werpt de Wbp belemmeringen op in de gegevensuitwisseling	semi-publiek
	het normatieve kader rond medisch wetenschappelijk onderzoek is lastig toepasbaar in de praktijk	semi-publiek
	door in de Wbp een regeling op te nemen over de verwerking van bijzondere gegevens is er sprake van overregulering	semi-publiek
	de interpretatievrijheid van de verantwoordelijke uit de Wbp wordt door onder meer onbekendheid te weinig gebruikt, waardoor onnodige belemmeringen ontstaan in de gegevensuitwisseling bij de ketenzorg	semi-publiek

Tabel 11. Knelpunten normatieve kaders

Uit de tabellen hierboven blijkt er twijfels zijn gerezen over de mate waarin de Wbp een voldoende helder en werkzaam kader verschaft voor de bescherming van persoonsgegevens. Hierbij gaat het om de complexiteit van de regelgeving, die tot kennis- en interpretatiemoeilijkheden in de praktijk leidt, en om de gelaagdheid van de regelgeving, die niet overal consequent is doorgevoerd. Als voorbeeld daarvan geldt de opname van een regime voor de verwerking van bijzondere persoonsgegevens in de Wbp, terwijl dergelijke regimes in plaats daarvan in sectorale wetgeving (konden) worden opgenomen.

De 'openheid' van het begrippenapparaat van de Wbp blijkt onder meer uit de manier waarop het doelbindingscriterium is vastgelegd in artikel 7 jo. artikel 9 Wbp: het legt een verband tussen het doel waarmee persoonsgegevens *verzameld* zijn en het doel waarvoor zij *verwerkt* worden. Dat de implementatie van de doelbinding in de Wbp in de praktijk weinig problemen oplevert, kan mogelijk worden verklaard door het gebrek aan (ook door de wet vereiste: de verdere verwerking moet niet onverenigbaar zijn) specificiteit van de geformuleerde doelstellingen ('het voeren van een effectieve financiële administratie'), zodat nieuwe verwerkingen al vrij snel aan het doelbindingscriterium zullen voldoen. Dat suggereert dat de Wbp kwetsbaar is voor de wijze waarop zij in de praktijk vorm krijgt. Hoewel dit uiteraard voor elke wet geldt, levert het open normenkader van de Wbp, zo lijkt het, extra kwetsbaarheid op.

Het instrumentarium van de Wbp is dermate algemeen geformuleerd, dat nieuwe wijzen van publiceren – met name op internet – strijd met de Wbp kunnen opleveren, terwijl andere vrijheden, zoals de vrijheid van meningsuiting, in het gedrang komen. De nationale wetgever heeft het evenwicht tussen grondrechten expliciet in zijn overwegingen bij de Wbp meegenomen. De Lindqvist-zaak lijkt vooralsnog een aanwijzing te zijn dat zo'n afweging van groot belang is, nu in die zaak in materiële zin het recht van vrije meningsuiting in zekere zin ondergeschikt is gemaakt aan het recht op bescherming van persoonsgegevens: een internetpublicatie die niet valt onder de uitzonderingen voor journalistieke, artistieke of literaire verwerkin-

gen moet worden gemeld, wat kan worden gezien als een moeilijk uitlegbare beperking van het beginsel van vrije meningsuiting.

De doelstellingen van de nationale wetgever op het gebied van normatieve kaders hebben betrekking op het vaststellen van een begrippenapparaat voor rechtsvorming en afweging van belangen, en een goede aansluiting daarvan bij het Nederlandse rechtsstelsel. Bij de analyse van knelpunten komt het beeld naar voren dat het opgestelde begrippenapparaat (a) onvoldoende houvast biedt in concrete situaties, (b) mogelijkheden tot interpretatie biedt die ten dele onbenut worden gelaten, en (c) in sommige gevallen tendeert naar overregulering door overlap met sectorale regelgeving.

8.3.3 Zelfregulering

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
nadere invulling, in verband met de verwerkingscontext, van materiële normen via zelfregulering	de gedragscode die van toepassing is op zorgverzekeraars vergroot de regeldichtheid, maar is kennelijk niet in staat adequaat te reageren op nieuwe ontwikkelingen binnen de zorgsector en geeft geen vorm aan het concept van zelfregulering	semi-publiek
	de inzet gemoeid met de opstelling van een gedragscode is bijzonder groot	algemeen
	in de publieke sector wordt weinig gebruik gemaakt van het instrument van de gedragscode	publiek
	de inzet die nodig is voor het opstellen van een gedragscode vormt een obstakel	privaat
	de plaatsbepaling van de gedragscode bij juridische geschillen is onduidelijk	privaat
	de gedragscode is geen breed gehanteerd reguleringsinstrument geworden, waar het wel als zodanig was bedoeld in de Wbp	privaat
bevorderen opstelling gedragscodes door inspraakmogelijkheden te schrappen		
ophelderen positie verantwoordelijken t.o.v. Cbp door opstelling bestuursrechtelijke rechtsgang	het is lastig de onafhankelijkheid van de FG te waarborgen	algemeen
invullen eigen verantwoordelijkheid van verantwoordelijken door instelling van FG	de instelling van een FG levert niet noodzakelijkerwijs een vergroting van de transparantie van gegevensverwerkingen op	algemeen
	het toezicht van het Cbp is onvoldoende afhankelijk van de aanstelling van een FG	algemeen
inspelen op eigen specifieke behoeften door het instellen van de meldingsplicht		

Tabel 12. Knelpunten zelfregulering

Uit literatuur blijkt dat knelpunten bij gedragscodes zich voordoen bij de inzet die gemoeid is met het opstellen van een gedragscode, de plaatsbepaling in het recht bij geschillen omtrent de betekenis van een gedragscode. Voorts doet een knelpunt zich voor bij het hanteren van de gedragscode als instrument voor zelfregulering ten aanzien van internetconsumenten.

Zelfregulering door middel van het opstellen van gedragscodes is een belangrijk doel van de Wbp. Met een sectorbrede gedragscode kunnen de algemene normen van de Wbp voor een bepaalde sector nader worden ingevuld en geconcretiseerd. Naast het kunnen concretiseren van de normen van de Wbp, is een gevolg van een aangenomen gedragscode dat het Cbp terugtreedt als eerstelijns toezichthouder. Deze terugtredende rol is nog sterker als met de gedragscode een vorm van onafhankelijke geschillenbeslechting in het leven is geroepen. Uit de literatuur blijkt dat knelpunten bij gedragscodes zich voordoen bij de inzet die gemoeid is met het opstellen van een gedragscode, en de plaatsbepaling in het recht bij geschillen omtrent de betekenis van een gedragscode. Voorts doet een knelpunt zich voor bij het hanteren van de gedragscode als instrument voor zelfregulering ten aanzien van internetconsumenten. Ten slotte zou de rol

van het Cbp bij het opstellen van gedragscodes te groot zijn om nog te kunnen spreken van zelfregulering of zelfs co-regulering, en zijn er tot nu toe weinig gedragscodes opgesteld.

De doelstellingen van de nationale wetgever op het gebied van zelfregulering hebben betrekking op de invulling van de relatief abstracte normen in de Wbp met concretere normen in bepaalde verwerkingscontexten, en de rol van het Cbp daarin als toezichthouder. Dit zou moeten geschieden door middel van gedragscodes, en de bevoegdheden van de functionaris gegevensbescherming. Knelpunten die hierbij aan de orde zijn, hebben onder meer betrekking op (a) de invulling van het instrument gedragscode, waarvan de inhoud te dicht bij de Wbp blijft, en het gebruik beperkt blijft, en (b) de invulling van de functionaris gegevensbescherming, waarvan de onafhankelijkheid nu onvoldoende gewaarborgd lijkt te zijn, en waarvan de aanstelling niet tot een andere rol van de toezichthouder leidt.

8.3.4 Transparantie en rechten van betrokkenen

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
vergroten van de transparantie van gegevensverwerkingen door toekenning van rechten en plichten, en het instellen van een toezichthouder	het Besluit kostenvergoeding bevat niet in alle gevallen een redelijke weerslag van de kosten die voor het realiseren van het kennisnemingsrecht noodzakelijk zijn	algemeen
	onvoldoende benutting mogelijkheden van het Vrijstellingsbesluit	algemeen
	omissies in correctie- en verzetsrechten maken het lastig voor betrokkenen om rechtsmiddelen te gebruiken	algemeen
	interpretatie van de begrippen die relevant zijn voor de informatieplichten stuit op problemen	algemeen
	te ruime werking van de meldingsplicht	algemeen
	de meldingsplicht levert onvoldoende bijdrage aan de transparantie van gegevensverwerkingen	algemeen
	het Vrijstellingenbesluit is complex en uitgebreid, en mede daardoor wordt het niet goed gebruikt, en wordt onterecht de toepasselijkheid van een vrijstellingsbepaling verondersteld	privaat
	de uiteenlopende implementatie van de meldingsprocedure in de Europese lidstaten leidt tot de onmogelijkheid deze meldingsplicht binnen een concern te harmoniseren	privaat
	de Wbp legt, in tegenstelling tot de richtlijn, een aan de verwerking voorafgaande informatieplicht op, die het bedrijfsleven meer tijd en inspanning kost dan	privaat
	de informatieplicht is vervat in een norm die met veel open begrippen is geformuleerd, wat tot interpretatiemoeilijkheden leidt	privaat
	het kennisnemingsrecht is nog weinig geconcretiseerd; door de onduidelijkheden over de interpretatie van 'persoonsgegeven' bestaat geen helderheid welke gegevens onder dat recht vallen	privaat
	er is te weinig duidelijkheid over de betekenis van art. 42 m.b.t. beslissingen op basis van geautomatiseerde gegevensverwerking	privaat
	de publicatieplicht voor de direct marketing branche is omslachtig en weinig zinvol	privaat
	meldingenregister is lastig bruikbaar, bevat voor dezelfde verwerkingen soms meerdere verantwoordelijken, en bevat vaak niet de meldingen die bij de functionaris gegevensbescherming zijn gedaan	privaat
	organisaties zijn onvoldoende toegerust voor voldoen aan kennisnemingsrecht betrokkenen	publiek

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
	van het inzage- en correctierecht wordt in de publieke sector in het algemeen niet veel gebruik gemaakt	publiek
	vaak ontbreken procedures en maatregelen om inzage- en correctierechten binnen de wettelijke termijnen op een zorgvuldige wijze te kunnen effectueren	publiek
	als gevolg van onduidelijkheid rond de verantwoordelijkheid voor de informatieplicht en de onbekendheid met deze verplichting laat de naleving hiervan binnen de semi-publieke sector te wensen over	semi-publiek
	effectuering van het kennisnemingsrecht wordt bij zowel de betrokkene als de verantwoordelijke belemmerd door een aantal praktische problemen als gevolg van het hoge abstractieniveau en te rigide normstelling	semi-publiek

Tabel 13. Knelpunten transparantie en rechten van betrokkenen

Het beeld dat uit een substantieel gedeelte van de relevante literatuur naar voren komt, is dat een aantal van de rechten en plichten uit de Wbp geringe naleving kent, of dat obstakels bestaan bij die naleving. Bij het algemene publiek lijkt de Wbp weinig bekend; met de bekendheid van de rechten en plichten die voortvloeien uit de Wbp is het niet veel beter gesteld. Die bekendheid met materiële rechten en plichten is natuurlijk belangrijker dan de kennis van het bestaan van een wet. Toch blijkt dat juist een in het oog springende norm als de informatieplicht (ook als die wordt uitgelegd naar z'n materiële inhoud) uit de Wbp bij weinig verantwoordelijken bekend is. Door het gebrek aan kennis van de Wbp bij burgers valt te verwachten dat rechten voortvloeiend uit de Wbp, met name het kennisnemingsrecht, maar in beperkte mate worden uitgeoefend. Dat beeld werd in bevestigd in de bijeenkomst met domeindeskundigen die in het kader van dit onderzoek is georganiseerd: op enkele op enkele uitzonderingen na (BKR, Dexia, Ministerie van Buitenlandse Zaken) lijkt er weinig gebruik te worden gemaakt van kennisnemingsrechten.

Van de informatieplicht van de verantwoordelijke richting betrokkene wordt geconstateerd dat deze vaak in te algemene zin wordt ingevuld: de doeleinden van de verwerking lenen zich bijvoorbeeld, net als bij de meldingsplicht, voor een generieke invulling. De onbekendheid van het instrumentarium van de Wbp kan niet aan de wet zelf worden geweten; voor de moeilijkheden bij de toepassing van de bepalingen omtrent rechten en plichten moet ten dele naar de wet, en ten dele naar het gebrek aan invulling van normen in lagere regelgeving en in de rechtspraak worden verwezen.

Geoordeeld naar de doelstelling van de wetgever, namelijk het vergroten van transparantie van gegevensverwerkingen door het toekennen van rechten en plichten, constateren wij dat het instrumentarium (a) te weinig bekendheid geniet voor een effectieve naleving; (b) in sommige gevallen onnodig complex is; (c) in sommige gevallen zijn doel voorbijschiet; en (d) de nadere invulling van het instrumentarium in lagere regelgeving en rechtspraak tot nu toe onvoldoende gestalte heeft gekregen.

8.3.5 Toezicht en rechtsbescherming

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
verbreden maatschappelijk draagvlak Cbp door toekenning bevoegdheden, en rechterlijke toetsing daarvan	er is betrekkelijk weinig geprocedeerd over de toepassing en werking van de Wbp, waardoor onzekerheid blijft bestaan over de invulling en concretisering van veel open normen in de wet	algemeen
	het ontbreekt bij de rechtsbescherming rondom de Wbp aan een eenduidige, laagdrempelige rechtsingang	algemeen
	systeem van gedifferentieerde rechtsbescherming is complex en maakt forumshopping mogelijk	algemeen

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
	de civiele rechtsingang voor het voldoen aan het correctierecht is niet eenduidig en hoogdrempelig	privaat
	de bekendheid van civiele rechters met de Wbp is beperkt	privaat
waarborgen onafhankelijkheid door het Cbp de status van zelfstandig bestuursorgaan te geven		
voorkomen belangenverstrengeling bij de toezichthouder door toetsing Cbp-bestuursreglement		
effectieve handhaving door het Cbp door bestuursdwang en bestuurlijke boetes		
laten aansluiten van de rechtsbescherming van betrokkenen bij het algemene recht		
versterken van de positie van verantwoordelijken t.o.v. het Cbp		
Knelpunten buiten doelstellingen nationale wetgever	**In literatuur geconstateerde knelpunten**	**Relevante sectoren**
	duur van het voorafgaand onderzoek is te lang	algemeen
	strafrechtelijke sancties in de Wbp sluiten niet goed aan bij de bestuursrechtelijke sancties in diezelfde wet	algemeen
	er wordt inhoudelijk geen invulling gegeven aan de algemene aanwijzingsbevoegdheid van de minister	algemeen
	de doorlooptijd van het voorafgaand onderzoek kan een knelpunt vormen, in het bijzonder voor samenwerkingsverbanden	publiek
	de verschillen tussen rechtsbescherming ten opzichte van besluiten in de publieke en private sector komen de rechtseenheid en de privacybescherming niet ten goede	publiek

Tabel 14. Toezicht en rechtsbescherming

De doelstellingen van de nationale wetgever hebben vooral betrekking op de positie van de toezichthouder. De geconstateerde knelpunten hebben daar geen direct verband mee, mede doordat wij ons terughoudend hebben opgesteld ten aanzien van het onderzoeken van knelpunten die direct op het Cbp betrekking hadden, nu niet het functioneren van de toezichthouder, maar de wet onderwerp is van de evaluatie. De knelpunten in het overzicht geven aan dat een ondubbelzinnige en laagdrempelige rechtsingang wordt gemist, en dat het systeem van gedifferentieerde rechtsbescherming als complex wordt ervaren.

Omdat in dit onderzoek het Cbp niet wordt geëvalueerd, kunnen wij niet aangeven of de nationale wetgever met betrekking tot de toezichthouder in haar bedoelingen geslaagd is. Daarbij verdient in elk geval wel de constatering aandacht, dat de rechtsbescherming door de rechter in de praktijk betrekkelijk weinig vorm heeft gekregen. Behalve in arbeidszaken en in een aantal specifieke financiële zaken (de zgn. 'Dexia-zaken') is de indruk dat er door particulieren cq. betrokkenen maar in beperkte mate een beroep wordt gedaan op de Wbp. Maar met name in het 'testen' van de verhouding tussen Cbp en verantwoordelijken voor de bestuurs- of civiele rechter is de Wbp in de praktijk nauwelijks uitgekristalliseerd. Motieven als vrees voor publicitaire repercussies (reputatiemanagement) en het vaak relatief geringe financiële belang van de specifieke zaak spelen daarbij mogelijk een rol.

De nationale wetgever heeft zich met betrekking tot het thema 'toezicht en rechtsbescherming' ten doel gesteld een maatschappelijk goed ingebedde, onafhankelijke en van voldoende bevoegdheden voorziene toezichthouder in het leven te roepen, waarbij verantwoordelijken van voldoende middelen worden voorzien om deze toezichthouder adequaat tegenwicht te bieden. We hebben in ons literatuuronderzoek en tijdens de expertbijeenkomsten geconstateerd dat (a) dit systeem van 'checks and balances' in de rechterlijke praktijk onvoldoende vorm heeft gekregen, (b) er een mogelijk hinderlijke differentiatie van rechtsingangen is bij het gebruik van deze wet, en (c) er relatief weinig geprocedeerd met inzet van de Wbp.

8.3.6 Internationale gegevensdoorgifte

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
bij ontbreken van beroep op uitzondering doorgifteverbod is bij wijze van 'noodklep' het instrument van een doorgiftevergunning	een doorgiftevergunning is onder sommige omstandigheden onnodig, maar wordt door het Cbp wel vereist	algemeen
instrumentarium waarmee zonder belemmering van het handelsverkeer wordt voorkomen dat de wet wordt omzeild of ontdoken	het ontbreken van een vergunningsvrijstelling bij gebruik van modelcontracten voor doorgifte van persoonsgegevens levert een administratieve last op	algemeen
	onduidelijkheid in de toepassing van uitzonderingsgronden op het verbod van doorgifte van gegevens leidt tot administratieve lasten, bijv. bij de doorgifte van persoonsgegevens van een vestiging binnen de EU naar een daarbuiten	privaat
	door het ontbreken van het zgn. Konzern Privileg kunnen human resource data binnen internationale concerns niet uitgewisseld worden zonder vergunning	privaat
	het 'safe-harbor'-principe is op elektronische markten geen garantie voor zorgvuldige omgang met persoonsgegevens	privaat
	de Wbp stelt onnodige eisen aan verwerking van persoonsgegevens in buitenlanden met een lager beschermingsniveau, nu deze verwerkingen langs twee routes in de Wbp gereguleerd worden	privaat

Tabel 15. Knelpunten internationale gegevensdoorgifte

In het thema 'internationale gegevensdoorgifte' heeft de nationale wetgever zich ten doel gesteld het handelsverkeer niet te belemmeren, en ontwijking van de wet niet nodig te laten zijn. Bij wijze van 'noodklep' is een voorziening ingebouwd die gegevensdoorgifte mogelijk maakt indien er geen beroep op een uitzondering op het doorgifteverbod kan worden gedaan. Deze doorgifte komt (met uitzondering van de gebieden waar de Wbp niet op van toepassing is, zoals op politiële gegevens) voornamelijk voor in de private sector, hoewel ook het ministerie van Buitenlandse Zaken ermee te maken heeft. Zodoende komen ook de voornaamste knelpunten voort uit de analyse van de private sector dat internationale doorgifte en verwerking in een buitenland onnodig moeilijk worden gemaakt.

De voornaamste knelpunten met betrekking tot internationale gegevensdoorgifte vloeien voort uit de analyse van de private sector, waarin internationale doorgifte en verwerking in een buitenland onnodig moeilijk worden gemaakt door onder meer (a) onduidelijkheden in uitzonderingsgronden, (b) het ontbreken van een speciaal regime voor internationale concerns, en (c) dubbele regulering van verwerkingen in buitenlanden met een lager beschermingsniveau.

8.3.7 Uitvoeringskosten

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
ruim gebruik van vrijstellingen op de meldingsplicht	de aan de meldingsplicht verbonden uitvoeringskosten zijn aanzienlijk	algemeen
eenvoudige melding daar waar deze wel vereist is		
verminderen kosten door mogelijk maken melding bij functionaris gegevensbescherming		
Knelpunten buiten doelstellingen nationale wetgever	**In literatuur geconstateerde knelpunten**	**Relevante sectoren**
	de uitvoeringskosten verbonden aan de doorgifteregels zijn aanzienlijk	algemeen
	de uitvoeringskosten verbonden aan de informatieplichten zijn aanzienlijk	algemeen
	de uitvoeringskosten verbonden aan het kennisnemingsrecht zijn aanzienlijk	algemeen
	bij de nulmeting van de administratieve lastendruk door de Wbp zou een te lage inschatting van de kosten zijn gemaakt	privaat
	meldingsformulieren en elektronische melding zijn onvoldoende eenvoudig	privaat

Tabel 16. Knelpunten uitvoeringskosten

Uit de evaluatie kan worden opgemaakt dat de uitvoeringskosten van de Wbp als knelpunt worden ervaren. De administratieve lastendruk is niet alleen aanzienlijk door de als kostbaar ervaren naleving van informatieplichten. Ook de eventuele aanstelling van een functionaris gegevensbescherming impliceert kosten. De doelstellingen van de wetgever, zoals een ruim gebruik van vrijstellingen op de meldingsplicht, het vergemakkelijken van de melding waar deze wel verplicht is, en het verminderen van kosten door het mogelijk maken van meldingen bij de functionaris gegevensbescherming, lijken alle slechts ten dele geslaagd.

De procedurele normen in de Wbp, inclusief de normen omtrent informatieplichten en de functionaris gegevensbescherming, zorgen voor een als aanzienlijk ervaren administratieve lastendruk. De instelling van een functionaris gegevensbescherming vermindert deze lastendruk niet, aangezien de administratieve verplichtingen intern blijven bestaan.

8.3.8 Technologie-onafhankelijkheid

Doelstellingen nationale wetgever	In literatuur geconstateerde knelpunten	Relevante sectoren
bereiken technologie-onafhankelijkheid van de regelgeving	de Wbp sluit niet aan bij technologische ontwikkelingen, waaronder de opkomst van het internet, spam, biometrie en nanotechnologie	algemeen
	de Wbp lijkt in zijn huidige vorm én toepassing niet in staat de technologische vooruitgang binnen de zorg adequaat te reguleren en normeren	semi-publiek
evenwicht tussen duidelijke regels en technologie-onafhankelijke regelgeving	de ontwikkeling en inrichting van nieuwe informatiesystemen vraagt om een constante nadere inkleuring van het normatieve kader van de Wbp; de onduidelijkheid die dit veroorzaakt hindert de ICT-innovatie binnen de zorg	semi-publiek

Tabel 17. Knelpunten technologie-onafhankelijkheid

De totstandkoming van de Wbp onder de toen net verschenen Nota Wetgeving op de Elektronische Snelweg[644] verklaart waarschijnlijk de nadruk die in de parlementaire geschiedenis is gelegd op die technologie-onafhankelijkheid, die immers in de betreffende Nota een belangrijk aandachtspunt vormde. Maar die beoogde technologie-onafhankelijkheid van de Wbp is aan kritiek onderhevig. Die kritiek houdt in dat

de focus van de wet wel degelijk uitgaat van de ten tijde van de totstandkoming heersende technologie, en te weinig rekening houdt met technologische ontwikkelingen die ten dele dan al in gang zijn gezet. De wet is dus wel abstract maar niet technologie-afhankelijk, en daardoor lastig toepasbaar op fenomenen als websites of RFID. Door de abstractie schiet de duidelijkheid van de normen uit de Wbp tekort.

De doelstelling van de wetgever om technologie-onafhankelijke én duidelijke normen te stellen lijkt, gezien de knelpunteninventarisatie, niet te zijn bereikt. Nieuwe technologieën konden niet naadloos in het regime van de Wet worden geïncorporeerd. Met ontwikkelingen zoals de profilering van individuen en gedistribueerde gegevensverwerking heeft de wetgever kennelijk geen rekening gehouden.

8.4 Drie perspectieven

Voor de nadere formulering van vragen met betrekking tot de werking van de Wbp is het nodig enige afstand te nemen tot de conclusies uit de vorige paragraaf, en deze te bezien in het licht van de drie perspectieven die op de achtergrond meespeelden in deze evaluatie: juridisch perspectief, handhaving en naleving, en beeldvorming. Op die manier kunnen we de geconstateerde frictie tussen doelstellingen en knelpunten van de Wbp gebruiken om een aantal belangrijke thema's die uit de eerste fase van de wetsevaluatie naar voren is gekomen tot een basis voor nadere vraagstelling voor de tweede fase van de wetsevaluatie te maken. De naar onze mening belangrijkste in de literatuur geconstateerde knelpunten met betrekking tot de drie perspectieven vatten wij hieronder samen:

Juridisch perspectief:

- Het gelaagde (Wbp, sectorale wetten) en gecompartimenteerde (bestuursrechtelijke, civielrechtelijke en strafrechtelijke dimensies) systeem voor de bescherming van persoonsgegevens is, in de poging aan te sluiten bij het Nederlandse rechtssysteem, zelf bijzonder complex geworden, en tendeert soms zelfs naar overregulering.
- Het begrippenapparaat en instrumentarium van de Wbp zijn als zodanig te abstract, en laten te veel ruimte voor interpretatie, om een helder kader te vormen voor de beoordeling van concrete vragen en situaties.

Daarmee wordt een belangrijke juridische doelstelling van de Wbp niet (ten volle) gerealiseerd: het vaststellen van een begrippenapparaat dat bruikbaar is voor rechtsvorming en voor de afweging van belangen.

Handhaving en naleving:

- De handhaving van de Wbp heeft een eenzijdig karakter door de nadruk op de bestuursrechtelijke rechtsgang; het beoogde stelsel van checks and balances krijgt beperkt vorm door het gebrek aan feitelijke rechterlijke toetsing van de beginselen die in de Wbp zijn vervat.
- De kwaliteit en werking van de zelfregulering in het kader van de Wbp laat te wensen over, onder meer door de rol van het Cbp, de onbekendheid van zelfreguleringsinstrumenten uit de Wbp, en de grote investeringen noodzakelijk voor goede zelfregulering.

Met betrekking tot het thema 'handhaving en naleving' geldt dat met name de doelstellingen van de rechterlijke toetsing van de aan het Cbp toegekende bevoegdheden, en de nadere invulling van materiële normen via zelfregulering maar beperkt gerealiseerd zijn.

Beeldvorming en bekendheid:

- Veel rechten en plichten van verantwoordelijken en betrokkenen die voortvloeien uit de Wbp worden niet uitgeoefend door een gebrek aan bekendheid van deze rechten en plichten bij het publiek en bij het midden- en kleinbedrijf en lagere overheden.

- Met betrekking tot de beeldvorming in de juridische literatuur constateren wij, naast beschrijvende literatuur over toepassing van de Wbp, een tamelijk eenzijdige nadruk op de knelpunten van de Wbp, een constatering die uiteraard ook haar weerslag heeft op de inhoud van dit rapport, dat immers voornamelijk van knelpunten spreekt.

Een van de centrale doelstellingen van de Wbp, namelijk het vergroten van de transparantie van gegevensverwerkingen door toekenning van rechten en plichten, en het instellen van een toezichthouder, lijkt daarmee (ten dele) onverwezenlijkt. Immers, als die rechten en plichten relatief onbekend zijn, zal daardoor de transparantie van gegevensverwerkingen niet kunnen worden verwezenlijkt.

8.5 Vraagarticulatie

Met het hierboven gegeven overzicht van de mate van realisatie van de voor de drie perspectieven behoren, en hun beperkte realisatie, gaan wij over tot de bepaling van relevante vragen voor de tweede fase van de evaluatie. Gezien de aard van de evaluatiebepaling in de Wbp moet in de empirische fase de nadruk liggen op het bepalen van de werking en doeltreffendheid van de Wbp. Naar aanleiding van de vele geconstateerde knelpunten, waaronder een gebrek aan werkzaamheid in bepaalde geledingen van de samenleving, ten dele voortvloeiend uit een gebrek aan kennis van de wet, zou wat ons betreft in het vervolgonderzoek ook op de vraag moeten worden ingegaan hoe de werking van de Wbp kan worden verbeterd, niet alleen met behulp van juridische en handhavingsinstrumenten, maar ook met voorlichting of andere beleids- of praktische instrumenten.

Met als vertrekpunt de plaatsing van de Wbp in het juridische systeem, die immers aan de basis staat van de werking en doeltreffendheid van het instrumentarium, starten wij vanuit de vraag hoe de Wbp te duiden is. De wet kent, door de inrichting van de toezichthouder en een deel van de rechtsbescherming, vooral een bestuursrechtelijke inslag, terwijl de civielrechtelijke en strafrechtelijke kanten van de wet beperkt zijn. Het commentaar dat op deze bestuursrechtelijke inslag wordt uitgeoefend, geeft evenwel geen sluitende argumenten waarom een civiele dan wel strafrechtelijke benadering te prefereren zou zijn. Vanuit systematisch oogpunt ligt immers een bestuursrechtelijke handhaving voor verticale werking van grondrechten voor de hand, en in horizontale verhoudingen is de weg naar de civiele rechter open. Het *ultimum-remedium*-karakter van het strafrecht, de heersende beweging om de sanctionering van overtredingen over te hevelen naar het bestuursrecht, en de beperkte handhavingscapaciteit van het Openbaar Ministerie maken ook de strafrechtelijke invalshoek niet tot de meest voor de hand liggende.

Na de vraag naar de doeltreffendheid van de plaatsbepaling van de Wbp in het juridische systeem volgt de vraag hoe het begrippenapparaat van de Wbp in juridische zin functioneert. De aard van dat begrippenapparaat blijkt onder meer uit de manier waarop het doelbindingscriterium is vastgelegd in artikel 7 jo. art 9 Wbp: het legt een verband tussen het doel waarmee persoonsgegevens *verzameld* zijn en het doel waarvoor zij *verwerkt* worden. Dat levert restricties op die vanuit het oogpunt van materiële bescherming niet kunnen worden gerechtvaardigd. Immers, voorzover doelbinding als een nuttig criterium kan worden beschouwd bij de verwerking van persoonsgegevens, levert een nieuwe doelstelling voor de verwerking van die gegevens, ten opzichte van de doelstelling bij het verzamelen ervan, niet noodzakelijkerwijs een inbreuk op de persoonlijke levenssfeer van de betrokkene op. Dat de implementatie van de doelbinding in de Wbp in de praktijk weinig problemen oplevert, komt wellicht door het gebrek aan specificiteit van de geformuleerde doelstellingen ('het voeren van een verantwoorde financiële administratie'), zodat nieuwe verwerkingen toch al vrij snel aan het doelbindingscriterium zullen voldoen. De door de wet vereiste specificiteit is beperkt: het verzameldoel moet welbepaald zijn en de verdere verwerking moet daarmee niet onverenigbaar zijn.

Dit suggereert dat de Wbp kwetsbaar is voor de wijze waarop zij in de praktijk vorm krijgt; hoewel dit uiteraard voor elke wet geldt, levert het open normenkader van de Wbp, zo lijkt het, extra kwetsbaarheid op.

Daarmee zijn wij beland bij de handhaving en naleving van de Wbp, die onder meer gekenmerkt wordt door een gebrek aan feitelijke rechterlijke toetsing. Zoals wij hierboven vermeldden, is met name de verhouding tussen Cbp en verantwoordelijken in de rechtspraak onvoldoende 'getest'. De motieven die wij gaven, zoals angst voor publicitaire repercussies en het vaak relatief geringe financiële belang van de specifieke zaak, spelen in de beperkte uitkristallisering waarschijnlijk een rol, maar geven naar onze mening onvoldoende verklaring.

In aansluiting op deze constatering over een gebrek aan rechterlijke toetsing, speelt ook de vraag naar de kwaliteit en werking van zelfregulering in het kader van de Wbp. Twee van de kristallisatiepunten voor de praktische vertaling van het abstracte normenkader van de Wbp zijn de gedragscode, en de rol van de functionaris gegevensbescherming. De perceptie van de rol van het Cbp als een instantie die te weinig ruimte laat voor werkelijke zelfregulering, onder meer door een gebrek aan 'afstand' tot deze reguleringmiddelen, doet de vraag rijzen of die afstand inderdaad ontbreekt, welke andere factoren een rol spelen bij het gedeeltelijk falen van zelfregulering, en hoe de werking van het zelfreguleringsinstrumentarium kan worden verbeterd.

Tot slot zijn daar de geconstateerde knelpunten gerelateerd aan beeldvorming en bekendheid. De werking van het instrumentarium van de Wbp, en daarmee het bereiken van de doelstellingen van die wet, staat of valt met de bekendheid van de rechten en plichten van de in de wet genoemde partijen. Daaraan lijkt het nodige te schorten. Bovendien is in een substantieel gedeelte van de literatuur, met name waar deze auteurs betreft die niet (meer) zijn verbonden aan het Cbp, een betrekkelijk negatieve houding aangetroffen ten aanzien van de Wbp.

De vele knelpunten maken het er niet gemakkelijker op om de vereiste inspanningen voor handhaving van de wet te verlangen van de betrokken partijen. Daarmee zijn wij beland bij het formuleren van vragen die naar onze mening aan de basis van de tweede fase van de wetsevaluatie zouden moeten staan. Het gaat om enkele vragen per thema, respectievelijk het juridische perspectief, handhaving en naleving, en beeldvorming en bekendheid.

Juridisch perspectief

Welke verbeteringen van de inhoud en toepassing van de Wbp zijn mogelijk binnen het kader van de richtlijn, om de wet als instrument ter bescherming van persoonsgegevens beter te doen functioneren ten aanzien van criteria zoals de werking en de reductie van administratieve lasten?

Bij de beantwoording van deze vraag kan, naast kwalitatief empirisch onderzoek door middel van interviews met wetgevingsjuristen, deskundigen in het domein van de Wbp, en deskundigen op het gebied van wetgevingsleer, gebruik worden gemaakt van de verbeteringssuggesties die zijn gedaan in de literatuur, en die zijn weergegeven in de sectorale hoofdstukken van dit rapport. Voor het verkrijgen van aanvullende suggesties is het aan te bevelen interviews te houden met advocaten, privacyadviseurs, privacyfunctionarissen (incl. functionarissen voor de gegevensbescherming) of andere deskundigen die ervaring hebben met toepassing van de Wbp in de praktijk. Om het bereik van de vraagstelling te beperken, kan gekozen worden voor de invulling van een specifieke plicht ten aanzien waarvan de knelpunten algemeen worden onderschreven, zoals de meldplicht of de informatieplichten, en voor een specifieke (sub)sector waarin die knelpunten het duidelijkst naar voren zijn gekomen.

Juridisch perspectief

Welke verbeteringen van de inhoud en toepassing van de Wbp zijn mogelijk binnen het kader van de richtlijn, om de wet als instrument ter bescherming van persoonsgegevens beter te doen functioneren ten aanzien van ontwikkelingen in informatie- en communicatietechnologie?

De indertijd beoogde technologie-onafhankelijkheid van de Wbp is aan kritiek onderhevig. Toepassing van de bepalingen van de wet op nieuwe technologieën, zoals internetdiensten, blijkt lastig. Onderzoek naar de aard van deze obstakels, door middel van interviews met experts en rechtsvergelijkend onderzoek, kan licht werpen op vereiste aanpassingen in de bepalingen van de Wbp. Daarbij zou qua focus een keuze gemaakt kunnen worden voor de on-line dienstverlening van het MKB en van lagere overheden.

Handhaving en naleving

Hoe komt het dat rechten en plichten die zijn neergelegd in de Wbp relatief weinig onderwerp zijn van rechterlijke toetsing, terwijl de toepassing van de Wbp is ingekleed met een systeem van 'checks and balances', waarvan die rechterlijke toetsing een belangrijk onderdeel uitmaakt?

De redenen die in dit rapport zijn weergegeven voor het gebrek aan feitelijke rechterlijke toetsing, vormen naar ons idee onvoldoende verklaring voor dat gebrek. Kwalitatief empirisch onderzoek (interviews) en juridisch onderzoek (rechtsvergelijking: hoe is het gesteld met rechterlijke toetsing van privacygerelateerde onderwerpen in andere landen van de Europese Unie) zouden moeten aangeven of er inderdaad aanvullende redenen zijn, en in welke gebieden deze te vinden zijn: bijvoorbeeld in het wettelijk kader, de invulling daarvan in lagere regelgeving en zelfregulering, en de rol van betrokken instituties. Daarbij zou de focus kunnen liggen op het handelen van grote ondernemingen, die immers over de middelen beschikken om rechterlijke toetsing te initiëren, maar daartoe niet zijn overgegaan.

Handhaving en naleving

Draagt de meldingsplicht daadwerkelijk bij aan de transparantie van gegevensverwerkingen, en welke oorzaken liggen ten grondslag aan de verschillen in de mate waarin instituties aan die meldingsplicht voldoen?

De meldingsplicht is onder andere geïntroduceerd als instrument om de verwerking van gegevens transparanter te maken. De rol die deze verplichting in de praktijk gespeeld heeft bij het bevorderen van die transparantie kan worden bepaald door kwalitatief empirisch onderzoek (vragenlijsten, interviews) naar de manier waarop verantwoordelijken vorm hebben gegeven aan deze verplichting, en of (en hoe) deze de omgang met persoonsgegevens heeft beïnvloed. Daarnaast kan worden getracht een duidelijker beeld te vormen van de oorzaken waardoor bedrijven, instellingen en overheden al dan niet aan deze verplichting voldoen.

Handhaving en naleving

Hoe heeft de relatie tussen Cbp en FG's vorm gekregen, en in hoeverre draagt de functionaris gegevensbescherming daadwerkelijk bij aan de transparantie van gegevensverwerkingen en in meer algemene zin aan de naleving van de wet?

De functionaris gegevensbescherming past in het model van zelfregulering binnen de kaders van de Wbp. De rol die dit instituut in de praktijk gespeeld heeft bij het bevorderen van de transparantie van gegevensverwerkingen kan worden bepaald door kwalitatief empirisch onderzoek (vragenlijsten, interviews) naar de rol (w.o. concrete bevoegdheden) van FG's in organisaties, het kennisniveau bij deze functionarissen, de mate waarin zij contacten onderhouden met het Cbp, en de inhoud van die contacten.

Beeldvorming en bekendheid

Hoe kunnen beeldvorming en bekendheid van de Wbp het beste onderzocht worden? Moet daarbij gekeken worden naar de wet en het daarin vervatte begrippenapparaat, of naar de betekenis van die wet voor bepaalde doelgroepen en bepaalde handelingen/thema's in het dagelijks leven van burgers en in het functioneren van instituties?

De Wbp raakt aan vele thema's in het leven van burgers en consumenten, en aan het handelen van overheden, instellingen en bedrijven. De weinige onderzoeken die naar beeldvorming en bekendheid van de Wbp zijn gedaan, hebben betrekking op begrippen die doorgaans rechtstreeks aan de wet zijn ontleend. Het is mogelijk dat dergelijke vragen over de Wbp te abstract zijn: bepaalde begrippen op het gebied van de bescherming van persoonsgegevens zouden onlosmakelijk verbonden kunnen zijn met thema's uit het persoonlijk leven van bijvoorbeeld burgers: als werknemer, als consument etcetera. Deze vraag gaat vooraf aan concreet onderzoek, en moet veronderstellenderwijs beantwoord worden in overleg met juristen, sociologen en voorlichtingsdeskundigen.

Beeldvorming en bekendheid

Welke rol is in het verleden weggelegd voor voorlichting over de Wbp? Welke rol speelt voorlichting in de mate van naleving van de Wbp? Kan – en zo ja: *hoe* kan – de voorlichting over de Wbp worden verbeterd?

In de beantwoording van deze vraag zou de nadruk moeten liggen op kwalitatief empirisch onderzoek (interviews) met de verantwoordelijken voor voorlichting bij het ministerie van Justitie, het College bescherming persoonsgegevens, een representatieve selectie van functionarissen gegevensbescherming, voorlichtingsdeskundigen en privacy-adviseurs en dergelijke. Deze vraag sluit direct aan op de vorige: indien voorlichting themagericht moet zijn – en niet gericht op de wet zelf – dan zal deze ook afhankelijk worden van doelgroepen.

Met deze opsomming van relevante onderzoeksvragen voor de tweede fase van de evaluatie Wet bescherming persoonsgegevens sluiten wij dit rapport af.

Leiden, Den Haag, 20 december 2006

Literatuur

A

ACTAL 2006
Adviescollege toetsing administratieve lasten, Brief 8 september 2006 aan het kabinet, Rl/AZ/2006/250, <www.actal.nl>.

Alberdingk Thijm 2003
Chr. Alberdingk Thijm, 'Tussen droom en daad: peer-to-peer en privacy', *P&I* 2003, p. 105-112.

ACT II 2004
Ambtelijke Commissie Toezicht II, Rapport van bevindingen betreffende de zelfevaluatie door het College Bescherming Persoonsgegevens (Cbp) van het toezicht op de verwerking van persoonsgegevens, 16 december 2004.

Ardenne 2003
E.M. van Ardenne, 'Het EMD, wie bewaakt de keerzijde van de sprong voorwaarts?', *P&I* 2003, p. 15-20..

B

Baeten & Janssen 2002
P. Baeten & L. Janssen, *Samenwerking en beroepsgeheim, Juridische mogelijkheden voor het uitwisselen van gegevens bij de aanpak van huiselijk geweld*, Utrecht: NIZW Uitgeverij, 2002.

Van den Bergen 2005
A.J.E. van den Bergen, 'De Wet bescherming persoonsgegevens in de financiële procespraktijk', *Tijdschrift voor financieel recht*, 2005/10, p. 296-306.

Berkvens 1983
J.M.A. Berkvens, 'Privacywet: deregulering of niet?', *Informatie* 1983-3, p. 42-45.

Berkvens 1992
J.M.A. Berkvens, 'Dynamische definities', in P. Van Hoogstraten (red.), *ISDN en privacy*, Amsterdam 1992, p. 41-54.

Berkvens 1994
J.M.A. Berkvens, 'EDI en privacyregels', in Van Esch & Prins (red.), *Recht & EDI*, Deventer 1994, p. 151-175.

Berkvens 2003
Berkvens, zoals aangehaald in J.E.J. Prins, 'Acht gesprekken over privacy en aanpalende belangen', in H. Franken et al., *Zeven essays over informatietechnologie en recht* Den Haag 2003.

Berkvens 2004a
J.M.A. Berkvens, 'Rechtspraak: De Lindqvist-case of de onbevlekte ontvangenis van persoonsgegevens', *P&I* 2004, p. 17-20.

Berkvens 2004b
J.M.A. Berkvens, 'Ontvreemde privacy', *Themis* 2004-5, p. 269.

Berkvens 2005a
J.M.A. Berkvens, 'Inzage, inzicht of overzicht', *P&I* 2005, p. 119-121.

Berkvens 2005b
J.M.A. Berkvens, 'Persoonsgegevens, wat zijn dat?', *P&I* 2005, p. 258-259.

Berkvens & van Esch 1994
J.M.A. Berkvens & R.E. van Esch, 'Het Burgerlijk wetboek als Wet persoonsregistraties', *Computerrecht* 1994-3, p. 93-100.

Berkvens & Prins 2002
J.M.A. Berkvens & J.E.J. Prins, *Privacyregulering in theorie en praktijk*, Kluwer: Deventer 2002.

Bijlsma & Homan 2003
L. Bijlsma & T.C.B. Homan, 'Toepassing Wbp door Kantonrechter bij ontslag werknemer; de Wbp ontslagen?', *Arbeid Integraal* 2003, p. 164-167.

Blok 2002
P.H. Blok, *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Den Haag: Boom Juridische Uitgevers 2002.

Blok 2003a
P.H. Blok, 'Is er privé-leven na de dood?', *NJB* 2003 nr. 6, p. 273-278.

Blok 2003b
P.H. Blok, 'Het beginsel van doelbinding', in Cuijpers, Van der Put & Terstegge (red.), *Privacy concerns*, Den Haag 2003, p. 45-59.

Blok 2004
P.H. Blok, 'Inkomens, internet en informationele privacy' *NTER* 2004, p. 30- 36.

Blok 2005a
P.H. Blok, 'Privacybescherming in alle staten', *Computerrecht* 2005, p. 297-304.

Blok 2005b
P.H. Blok, 'De waarde van de omnibuswet', *P&I* 2005, p. 246-252.

Bruin & Terstegge 2006
K.J. Bruin & J.H.J. Terstegge, 'Privacy Officers in NGFG-land' , *P&I* 2006, p. 185-186.

Bruning 2006
M. Bruning, *Over sommige kinderen moet je praten. Gegevensuitwisseling in de jeugdzorg*, oratie 11 april 2006.

C

RCO 2003
Council of Central Employers' Organisations. Findings of the RCO Committee on Privacy on the evaluation of the European Privacy Directive (95/46/EC) <http://ec.europa.eu>.

Covers, Hardam & Nouwt 2004
J.F.M. Corvers, E. Hardam & J. Nouwt, 'Aanbesteding project Psychiater & Kwaliteit', *Journaal Privacy Gezondheidszorg*, 5(10), p. 222-227.

Cuijpers 2003
C.M.K.C. Cuijpers, 'Evaluatie van de richtlijn', in Cuijpers, Van der Put & Terstegge (red.), *Privacy concerns*, Den Haag 2003.

Cuijpers 2004
C.M.K.C. Cuijpers, *Privacyrecht of privaatrecht*, (diss. UVT) Nijmegen 2004.

Cuijpers 2006
C.M.K.C Cuijpers, *Verschillen tussen de Wbp en richtlijn 95/46/EG en de invloed op de administratieve lasten- en regeldruk*, 22 juni 2006 <www.actal.nl>.

D

Van Daal 2006
E.S.A.M. van Daal, 'Privacy-aspecten van MedDos: een elektronisch medicatiedossier', *JPG* 2004, p. 214.

Dijkstra, Poort en van Zeevaart 2006
M. Dijkstra, B. Poort en A van Zeevaart, verslag van een ELSA-congres over 'Privacy en de weg naar de informatiesamenleving', in *P&I* 2006-2, p. 75.

Dubbeld 2006
L. Dubbeld, 'Privacybeleid van Nederlandse telemedicine websites', *P&I* 2006-3, p. 132-136.

E

Van Eck 2002
B.M.A. van Eck, 'SUWI: chaos van gegevens achter één loket?' *P&I* 2002, p. 65-71.

E-commerce Platform, Persbericht 13 november 2001, aangehaald in *P&I* 2002, p. 34-35.

Economic Evaluation of the Data Protection Directive 95/46/EC (Final Report) May 2005.

ECP.nl, 'rapport privacyrechtelijke aspecten RFID', mei 2005.

EOS Gallup 2003
EOS Gallup Europe, Data protection in the European Union, (FLASH EuroBarometer nr. 147) december 2003.

Esch 2005
R.E. van Esch 'Wordt hulpverlening belemmerd door de Wbp?', *Computerrecht* 2005, p. 38.

Van Essen 2003
J.M. van Essen, 'Uitvoeringsproblemen van de Wet bescherming persoonsgegevens', *Ondernemingsrecht* 2003, p. 360-367.

Europe and the global information society - Recommendations to the European Council, Brussel, 26 mei 1994.

Even 2003
J.H. Even, 'Reactie op "De wet bescherming persoonsgegevens in de arbeidsrechtpraktijk toegepast"', *Arbeidsrecht* 2003, p. 37-39.

F

FNV 2003
Federatie Nederlandse Vakbeweging, Opinion of the Netherlands Trade Union Federation on European Directive No 95/46/EC < http://ec.europa.eu>.

G

Gevers 1999
J.M.K. Gevers, 'Nieuwe privacywetgeving en de gezondheidszorg', *Sociaal recht* (1999) 3, p. 66.

Goderie & Steketee 2005
M. Goderie & M Steketee, 'Bemoeizorg voor multiproblemgezinnen in relatie tot privacybescherming', *JPG*, september 2005.

Graaf 1987
De Graaf, *Privacy en persoonsgegevens*, Lelystad 1987.

Groothuis 2005
M.M. Groothuis, *Beschikken en digitaliseren*, (Diss. Leiden) Den Haag 2005

H

Hees 2006
R. Hees e.a., 'Het gevaar van diagnosebehandelcombinaties' *Tijdschrift voor de Psychotherapie* 2006 (32) nr. 2, p.115-117.

De Heij 2001
A.C.M. de Heij, 'Het WBP-vrijstellingsbesluit', *P&I* 2001-2, p. 59-63.

De Hert 2000
P. de Hert, 'Kenbaarheid van bedrijfscontrole op e-mail en internetgebruik: factoren die spelen bij de chaos rond dit leerstuk', *P&I* 2000-1, p. 26-30.

De Hert & Gutwirth 2004
P. de Hert & S. Gutwirth, 'Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek', in E.R. Muller (red.), *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn 2004, p. 587-631.

Heuver 2003
J.W. Heuver, 'Credit scoring en privacy', *Rechtshulp* 2003, p. 55-61.

Holvast 1996
J. Holvast, *Persoonsgegeven of niet: dat is de vraag*, Alphen aan den Rijn/Diegem 1996.

Holvast 1999
J. Holvast, 'Privacyregels voor EDI-berichten', in *Toepassing van privacyregels op elektronische berichten*, Deventer 1999.

Holvast 2002a
J. Holvast, '24th Data Protection Commissioners Conference', *P&I*, 2002-6, p. 260-261.

Holvast 2002b
J. Holvast, 'Wetenschappelijk onderzoek en privacy', in J.E. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002, p. 370 e.v.

Holvast 2004
J. Holvast, 'Awb en bescherming van persoonsgegevens (Praktijkdossiers Algemene wet bestuursrecht)', Deventer 2004.

Holvast 2005a
J. Holvast, annotatie bij Rb. Amsterdam 19 mei 2005 in *Computerrecht* 2005/6, p. 323-327.

Holvast 2005b
J. Holvast, 'Wet bescherming persoonsgegevens: privacywet of een wet die gegevens beschermt?', *P&I* 2005-5, p. 242-245.

Holvast 2005c
J. Holvast, 'Interview met Jacob Kohnstamm', *P&I* 2005-3, p. 114-119.

Holvast 2005d
J. Holvast, 'De aanmeldplicht, een overbodige bepaling?', *P&I* 2005-6, p. 208-211.

Holvast, Merkus & Michels 2004
J. Holvast, S. Merkus en G. Michels, De staat van de privacybescherming van de burger, in: *P&I* 2004, p. 249 e.v.

Holvast & Prins 2003
Holvast en J.E.J, Prins, 'Acht gesprekken over privacy en aanpalende belangen', in H. Franken et al, *Zeven essays over informatietechnologie en recht*, Den Haag 2003.

Holvast & Rodrigues 2005
J. Holvast & P.R. Rodrigues, 'De gevoeligheid van bijzondere gegevens', *P&I* 2005-6, p. 263-267.

Hooghiemstra 2002a
T. F. M. Hooghiemstra, Privacy bij ICT in de zorg, *ZM magazine*, november 2002, nr. 11.

Hooghiemstra 2002b
T.F.M. Hooghiemstra, *Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg*. Den Haag: Cbp, A&V 2002 nr. 26.

Hooghiemstra 2004
T.F.M. Hooghiemstra, 'Privacy bij ICT in de zorg. Inzichten ervaringen en vooruitzichten', *JPG* 2004, p. 208-212.

Van der Horst 2002
R.J.M. van der Horst, 'De Wet bescherming persoonsgegevens, gevolgen voor de organisatie en de automatisering', in J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002.

Van den Hoven van Genderen & Gilhuis 2003
R. van den Hoven van Genderen & A. Gilhuis, Persoonsgegevens door gemeentelijke sociale diensten. Een probleem? *PS Documenta* 2003 nr. 18, p. 2140-2156.

Hustinx, 2004
P.J. Hustinx, 'Bescherming van persoonsgegevens op koers', *Themis* 2004-5, p. 270-272.

Hustinx 2005
P.J. Hustinx, 'Data Protection in the European Union', *P&I* 2005 p. 62-65.

I

IGZ, 'ICT in ziekenhuizen', augustus 2004.

Implementation Report
First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003)265 final, Brussel, augustus 2003.

Inspectie jeugdhulpverlening 2003
Rapport inspectie jeugdhulpverlening en jeugdbescherming e.a., 'Horen, zien, niet zwijgen', 2003.

J

Jager 2003
M.J Jager, 'De Wet bescherming persoonsgegevens in de arbeidsrechtspraktijk toegepast', *Arbeidsrecht* 2003, p. 10-16.

Jakimowicz & Borrat i Frigola 2006
C. Jakimowicz & M. Borrat i Frigola, 'Uitwisseling van persoonsgegevens naar landen binnen en buiten de Europese Unie', *ArbeidsRecht* 2006, p. 25-33.

K

Kabel 1997
J.J.C. Kabel, 'Bescherming van persoonsgegevens en de openbare informatievoorziening', *Mediaforum* 1997-5, p. 76-80.

Van der Klaauw-Koops & J.E.J. Prins 2002
F.A.M van der Klaauw-Koops & J.E.J. Prins, 'Internationale privacyregulering: belangen, problemen en mogelijkheden' in J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002.

Kielman & Koelewijn 2000
H.H. Kielman & W.I. Koelewijn, Meer maatregelen, minder risico, *IT Monitor* september 2005 nr. 8.

Koekkoek 2000
Koekkoek (red.), *De Grondwet*, Deventer 2000.

Kohnstamm & Fontein 2006
J. Kohnstamm en M.A.H. Fontein, 'Interpretatie en harmonisatie: het werkprogramma van de Artikel 29-werkgroep voor 2006 en 2007', *P&I* 2006, p. 127-128.

Koning & de Vries 2003
M. de Koning & H. de Vries. 'Databankenrecht en privacyrecht', *P&I* 2003, p. 52-58.

Kolk & Verbruggen 2002
D.J. Kolk & M. Verbruggen, 'Het verborgen bestaan van de Wet bescherming persoonsgegevens', *Arbeidsrecht* 2002, p. 3-10.

Kooijmann 2006
M.J.J. Kooijman, 'Nieuwe privacycode Zorgverzekeraars', *JPG* 2006, nr. 3.

Kranenborg 2004
H. Kranenborg, 'Pas op met wat je op je homepage zet! Publicatie van persoonsgegevens op Internet beschermd door Europese regelgeving', *NJCM-bulletin* 2004, p. 415 e.v.

Kroes 2003
Q. Kroes, 'De Wbp in het algemeen', in Cuijpers, Van der Put & Terstegge (red.), *Privacy concerns*, Den Haag 2003, p. 24-29.

Kuitenbrouwer 2002
F. Kuitenbrouwer, 'Privacy: een historisch vergelijkend overzicht', in J.M.A. Berkvens & J.E.J. Prins (red.), *Privacyregulering in theorie en praktijk*, Kluwer Deventer 2002.

L

Lacevic & Zondag 2004
D. Lacevic & W.A. Zondag, 'Ontslag wegens e-mail- en internetmisbruik op de werkvloer, mede in rechtsvergelijkend perspectief', *Arbeid Integraal* 2004, p. 91-98.

Lieon & van Munster-Frederiks 2004
S. Lieon & M. Th. Van Munster-Frederiks, *De zieke werknemer en privacy*, Den Haag 2004

Lodder e.a. 2004
A.R. Lodder, H.W.K. Kaspersen, M. Briet, D.F. Groenevelt, MC Steeman, and C.W. Suen, *Spam, spammer, ... Analyse van het recht en de techniek rond elektronische ongevraagde commerciële communicatie, in het bijzonder via email*, Den Haag 2004.

Lowentahl & Wijenbergh 2004
Jan-Roel Lowenthal, John Wijenbergh, 'Lezen zonder zien; een verkenning van security issues rondom het gebruik van RFID', *Informatiebeveiliging*, 2004.

Lucieer 2006
V.C. Lucieer, 'Invoering van het burgerservicenummer in de zorg,' *JPG* 2006 nr. 5.

M

Maring 2003
H. Maring, 'Reactie op FAQ: Privacy na de dood?', *JPG* 2003, nr. 3, p. 8.

Marbus 2005
R.C.P. Marbus, 'Nanotechnologie en privacy: kleine technologie met grote gevolgen', *P&I* 2005, p. 57-61.

Merkus 2002
S.H. Merkus, 'Gevolgen van de Wbp voor due diligence-onderzoek', *P&I* 2002, p. 14-18.

Merkus 2004
S.H. Merkus, 'Toepassing van art. 76 en 77 lid 2 Wbp', *P&I* 2004, p. 12-16.

N

Nagel 2006
K.P. Nagel, 'Privacy vanuit consumenten bezien'. *P&I* 2006, p. 268-270.

Nas 2005
S. Nas, 'Iedereen een chippie in zijn arm? RFID-labels en de wolk van gegevens', *P&I* 2005, p. 105-109.

NEN Normcommissie Informatiebeveiliging in de Zorg, <www.nen.nl>.

Nouwt 1999
S. Nouwt, 'Privacyregels voor Internetberichten' in *Toepassing van privacyregels op elektronische berichten*, Deventer 1999.

Nouwt 2003a
J. Nouwt, Vaststelling identiteit bij inzageverzoek, *JPG*, 2003, nr. 5, 10-11.

Nouwt 2003b
J. Nouwt, 'Advies Conceptbesluit tot wijziging Besluit SUWI', *JPG*, 2003 nr. 5, p. 2-3.

Nouwt 2003c
J. Nouwt, 'Cbp kondigt sancties aan voor niet-melden', *JPG* 2003, nr. 4, p. 12-13.

Nouwt 2003d
J. Nouwt, 'Afspraak VWS, ZN en Cbp over gebruik DBC's door zorgverzekeraars', *JPG* 2003, nr. 9, p. 2.

Nouwt 2003e
J. Nouwt, 'Antwoord op FAQ 2003/5: Inzage door nabestaanden', *JPG* 2003, nr. 7, p. 10.

Nouwt 2003f
J. Nouwt, 'Kinderen, internet en privacy', *P&I* 2003, p. 52-58.

Nouwt 2004
J. Nouwt, 'Informatie-uitwisseling bij ketenzorg', *JPG* 2004, p. 232.

Nouwt 2005
J. Nouwt, *Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet*, Den Haag 2005.

NVO-NCW, Brief d.d. 15 december 2004, kenm. 04/15.098/Gf/CV.227.

O

Overkleeft-Verburg 1995
G. Overkleeft-Verburg, De *Wet persoonsregistraties*, (diss. KUB), Zwolle 1995.

P

Ploem 1999
M.C. Ploem, 'Informationele privacy in de gezondheidszorg: algemene privacywetgeving overbodig?' *P&I* 1999.

Ploem 2001
M.C. Ploem, 'Vertrouwelijkheid van medische gegevens: continuïteit en ontwikkeling', *Tijdschrift voor Gezondheidsrecht*, 2001, p. 34-44.

Ploem 2004
M.C. Ploem, *Tussen privacy en wetenschapsvrijheid. Regulering van gegevensverwerking voor medisch wetenschappelijk onderzoek*. (Diss. Utrecht) Den Haag 2004.

Van de Pol 1998a
U. van de Pol, 'De rol en het sanctiebeleid van de registratiekamer nu en straks', *P&I* 1998, p. 15-19.

Van de Pol 1998b
U. van de Pol, 'Geen privacybescherming zonder publiciteit', *Mediaforum* 1998, p. 135.

Van de Pol 2000
U. van de Pol, 'Toekomstig toezicht op bescherming van persoonsgegevens: van Registratiekamer naar College bescherming persoonsgegevens', *NJCM-Bulletin* 2000, nr. 7/8, p. 1141-1157.

Van de Pol 2003
U. van de Pol, ' Juridische grenzen', *NRC Handelsblad*, 13 september 2003.

Van de Pol & Van Seumeren 2004
U van de Pol & N. van Seumeren, 'Sociale zekerheid: privatisering en deregulering gaan niet samen', *NRC Handelsblad*, 1 november 2004.

Van der Pol 2006
S.J.T. van der Pol. 'Toets of de Wbp binnen Vitalis wel vitaal is: een onderzoek naar de mate waarin de Wbp wordt nageleefd binnen de Vitalis Zorggroep', *P&I* 2006, p. 110-114.

Van Pomeren 2006
M.J. van Pomeren, 'Het gebruik van persoonsgegevens in de gemeentepraktijk', De *Gemeentestem* 2006, p. 333 e.v.

Prins 1998
C. Prins, 'De bescherming van persoonsgegevens: de betrokkene betrokken', *P&I* 1998, p. 11-14.

Prins 2003
J.E.J. Prins, 'Acht gesprekken over privacy en aanpalende belangen', in H. Franken e.a., *Zeven essays over informatietechnologie en recht*, Den Haag 2003.

Prins 2004a
J.E.J. Prins, 'Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy', *Justitiële Verkenningen*, 2004-8, p. 34-47.

Prins 2004b
J.E.J. Prins, 'The Propertization of Personal Data And Identities', *EJCL*, Vol. 8.3 October 2004 <www.ejcl.org>.

Prins 2006
C. Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity' in: *The Future of the Public Domain - Identifying the Commons in Information Law*, The Hague 2006.

Prins et al. 1996
Prins et al, *De WPR als zon maan of ster*, Alphen aan de Rijn 1995.

Prins & Berkvens 2002
J.E.J. Prins & J.M.A. Berkvens, 'De Wet bescherming persoonsgegevens', in Prins & Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002.

Projectgroep Wet Bescherming Persoonsgegevens, *Lasten van de Wbp. Rapportage aan de Commissie Administratieve Lasten*, Den Haag, 19 april 1999.

Van der Putt 2003
P. van der Putt, 'De verantwoordelijke en de bewerker', in Cuijpers, Van der Put & Terstegge (red.), *Privacy concerns*, Den Haag 2003, p. 31-34.

PvG. 'Implementatie van de Wbp: de resultaten van Prismant', *JPG* juni 2003.

Q

Van Quathem 2005
K. van Quathem, 'Controlling personal data - the case of clinical trials', *P&I* 2005, p. 155-161.

R

Rank & Haasjes 2005
W.A.K. Rank & A.J. Haasjes, 'Misbruik van de Wbp in civiele procedures tegen financiële instellingen', *Tijdschrift voor financieel recht*, 2005/12, p. 370-379.

RCO 2003
Council of Central Employers' Organisations. Findings of the RCO Committee on Privacy on the evaluation of the European Privacy Directive (95/46/EC) (opinie), http://ec.europa.eu (publicatiedatum onbekend).

Van Ringelestijn 2006
T. van Ringelestijn, Privé-informatie nog steeds makkelijk te koop; Kopers persoonsgegevens niet vervolgd, (webartikel), <www.netkwesties.nl> 1 juli 2006.

S

Schermer 2005
B. Schermer 'Wat is RFID?' in G-J. Zwenne & B. Schermers (red.) *Privacy en andere juridische aspecten van RFID*, Den Haag 2005.

Schilder 2002
A.E. Schilder, 'Privacyregulering en de Awb', in J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002.

Schildmeijer, Samson & Koot 2005
R. Schildmeijer, C. Samson & H. Koot, *Burgers en hun privacy. Opinie onder burgers*, TNS NIPO februari 2005

Schmidt 2006
A.H.J. Schmidt, 'Is dit wel het goede moment om er het bijltje bij neer te gooien?', *Mediaforum* 2006-9, p. 245.

Van Schoonhoven 2006a
J.P. van Schoonhoven, 'Inzage bij banken: een recht te ver?', *Computerrecht* 2006-4, p. 200-205.

Van Schoonhoven 2006b
J.P. van Schoonhoven, 'Inzage bij banken; een recht te ver?', in A.W. Duthler (red.), *ICT: vierde macht in de Politica?*, Den Haag 2006, p. 81-91.

Schreuders & Blok 2002
E. Schreuders & P. Blok, 'Privacyregels en de Wbp op het internet', in J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002.

Schreuders & Gardeniers 2005
E. Schreuders & H. Gardeniers, 'Materiële normen: de kloof tussen de juridische normen en de praktijk', *P&I* 2005, p. 260-262.

Van Seumeren 2005
N. van Seumeren, 'Privatisering en deregulering gaan niet goed samen als het gaat om de bescherming van de persoonlijke levenssfeer', *P&I* 2005 ,p. 15-19.

Smeets 2004
A.H.C.M. Smeets, Camera's in het publieke domein - Privacynormen voor het cameratoezicht op de openbare orde, Cbp december 2004.

Smits 2006
F. Smits, ' De toelaatbaarheid van drugs- en alcoholtesten in de werkrelatie', *P&I* 2006, p. 115-120.

Straetmans 2004
G. Straetmans, 'De zorgverzekeraars en privacy', *JPG* 2004, p 47-51.

Swedish It Law Observatory, *An Abuse Model?*, Report S/98, 1998.

T

TdB, 'Reactie op FAQ Bemoeizorg', *JPG* 2001, 5-6.

Terhorst 2006
A.M. Terhorst, 'Van Esch gaat te gemakzuchtig om met de WBP', *Computerrecht* 2006, p. 42.

Terstegge 2000
J.H.J. Terstegge, 'Van de regen in de drup', *NTBR* 2000-8, p. 243-251.

Terstegge 2002
J.H.J. Terstegge, 'Home Country Control - Improving privacy compliance and supervision', *P&I* 2002, p. 257-259.

Terstegge 2005
J. Terstegge, 'Toepassingen en toekomst van RFID', in G-J. Zwenne & B. Schermers (red.) *Privacy en andere juridische aspecten van RFID*, Den Haag 2005.

Thijssen, 2002
M.B.J. Thijssen, 'Wet Bescherming Persoonsgegevens in concernverband' , *Computerrecht* 2002-2, p. 84-88.

Thijssen, 2005
M.B.J. Thijssen, 'Grensoverschrijdend gegevensbeschermingsrecht', *P&I* 2005, p. 110-113.

Titulaer 2006
Z. Titulaer, 'Ontwikkelingen in FG-land', *P&I* 2006, p. 23-24.

TNS NIPO 2006
TNS NIPO, De naleving en beleving van de informatieplicht onder organisaties in Nederland, februari 2006.

U

V

Van Veen 2003
E-B van Veen, 'Gecodeerde gegevens bij wetenschappelijk onderzoek: een begripsverheldering', *P&I* 2003, p. 259-262.

VNO-NCW 15 december 2004, brief aan de Minister van Justitie, 04/15.098/Gf/CV.227.

Verhey 1997
L.F.M. Verhey, 'EG-richtlijn bescherming persoonsgegevens: uitgangspunten en hoofdlijnen', *NJCM-Bulletin*, jrg. 22 (1997), nr. 3, p. 239-256.

Versmissen & de Heij 2002
J.A.G. Versmissen, A.C.M. de Heij, 'Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-structuur van de overheid, Cbp juli 2002.

Versmissen, Schinkel & Kraai 2006
K. Versmissen, M. Schinkel & E. Kraai, Publicatie van persoonsgegevens op internet, Cbp mei 2006.

De Vries 2006
H.H. de Vries, 'Grensoverschrijdende gegevensbescherming', *P&I* 2006, p. 265-267.

W

Van der Wel 2005
J.A. van der Wel, 'Spoort de medische praktijk nog wel met de wettelijke regeling voor het medische beroepsgeheim', *JPG*, april 2005 nr. 3.

Van der Wel & Homma 2003
J. van der Wel en N. Homma, 'Gegevensbeveiliging aan alle kanten lek' , *Automatisering Gids* 2003 nr. 5.

Winkelhorst 2005
R.C. Winkelhorst, 'Privacy en zoekmachines', *P&I* 2005, p. 146-154.

Winkelhorst & van der Linden-Smith 2004
R.C. Winkelhorst & T. van der Linden-Smith, 'Persoonsgegevens op Internet. Een (ver)melding waard?', *NJB* 2004, p. 627-631.

WODC, Actualisatie nulmeting AL Ministerie van Justitie. Onderzoek naar de Administratieve Lasten voortvloeiend uit de regelgeving van het Ministerie van Justitie op de peildatum 31 december 2002, Den Haag 2003.

X

Y

Z

De Zeeuw 2005
J. De Zeeuw, 'De toekomst van de functionaris voor de gegevensbescherming', *P&I* 2005, p. 214-216.

Van der Zijde 2006
M.E. van der Zijde, 'Tegenstrijdigheid tussen de opt-in regels?', *P&I* 2006, p. 121.

Zwenne 2003
G-J. Zwenne, 'Boekbespreking', *Themis* 2003-6, p. 322-323.

Zwenne 2004
G-J. Zwenne, 'Bodil Lindqvist. Noot bij EHvJ 6 november 2003', *JAVI* 2004-2, p. 66-69.

Zwenne & Webbink 2006
G-J. Zwenne & J. Webbink, 'De winstverdubbelaar en de Wbp: over de reikwijdte en inhoud van het kennisnemingsrecht van art. 35', *P&I* 2006, p. 2-8.

Rechtspraak

Europees Hof van Justitie

EHvJ 4 december 1986, 205/84, *PbEG* 1986, p. 3755.

EHvJ 10 mei 1995, zaak C-384/93, NJ 1995, 703.

EHvJ 6 maart 2001 (Connolly/Commissie), C-274/99P, r.o. 37.

EHvJ 20 mei 2003 (Österreichischer Rundfunk), C-465/00, C-138/01 en C-139/01.

EHvJ 6 november 2003, (Bodil Lindqvist) C101/01

EHvJ 30 mei 2006, zaken C-317/04 en C-318/04.

Europees Hof Rechten van de Mens

EHRM 17 januari 1970, 2689/65 (Delcourt).

EHRM 6 september 1978, 5029/71 (Klass).

Hoge Raad

Hoge Raad 21 april 2001, *NJ* 2001, 421 (Wennekes lederwaren).

Afdeling Bestuursrechtspraak Raad van State

ABvRS 3 maart 2004, *LJN* AO4783.

ABvRS 7 april 2004, *LJN* AO7115 (NVH/Cbp).

ABvRS 21 september 2005, *LJN* AU2998.

ABvRS 22 februari 2006, *LJN* AV2256.

ABvRS 12 juli 2006, *LJN* AY3726.

ABvRS 11 augustus 2004, *JB* 2004/325, m.nt. G. Overkleeft-Verburg.

ABvRS 12 mei 2004, *JB* 2004/251, m.nt. G. Overkleeft-Verburg.

ABvRS 12 juli 2006, m.nt. G. Overkleeft-Verburg.

ABvRS 12 januari 2005, *JB* 2005/75 m.nt. G. Overkleeft-Verburg.

ABvRS 8 december 2004, *JB* 2005/26 m.nt. G. Overkleeft-Verburg.

ABvRS 15 juni 2005, *JB* 2005/230, m.nt. G. Overkleeft-Verburg.

ABvRS 14 juli 2004, *JB* 2004/297, m.nt. G. Overkleeft-Verburg.

Gerechtshof

Gerechtshof Arnhem 11 juli 2006, zaaknummer 120/2006.

Gerechtshof Leeuwarden, 4 december 2002, *LJN* AF1344.

Rechtbank

Rechtbank Leeuwarden, 3 mei 1993, *NJ* 1994.

Rechtbank Maastricht, 5 december 2003, *LJN* AO0044.

Rechtbank Den Haag, 3 maart 2004, *LJN* AO48801.

Rechtbank Den Bosch, 31 maart 2004, *LJN* AT3148.

Rechtbank Den Haag, 7 april 2004, *LJN* AO8756.

Rechtbank Amsterdam, 19 mei 2005, *LJN* AT5858.

Rechtbank Groningen, 16 juni 2005, *LJN* AT9375.

Rechtbank Utrecht, 17 augustus 2005, *LJN* AU1068.

Rechtbank Amsterdam, 10 november 2005, *LJN* AU6428.

Rechtbank Arnhem, 10 mei 2006, *LJN* AX1994.

Rechtbank Arnhem, 5 oktober 2006, *LJN* AX1994.

Rechtsbank 's Hertogenbosch, 18 januari 2005, *LJN* AT0462.

Voorzieningenrechter Rechtbank

Vzr. Rechtbank Amsterdam, 11 december 2003, *LJN* AN9893.

Artikel 29 werkgroep

Art. 29 Werkgroep 2001
Art. 29 Werkgroep, Opinion 8/2001 on the processing of personal data in the employment context, 13 september 2001, DG Markt 5062/01, WP 48.

Art. 29 Werkgroep 2002
Art. 29 Werkgroep, Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU, WP56, 30 mei 2002.

Art. 29 Werkgrop 2005a
Art. 29 Werkgroep, Working document on data protection issues related to RFID technology, WP105, 19 januari 2005.

Art. 29 Werkgroep 2005b
Art. 29 Werkgroep, Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995, WP114, 25 november 2005.

Art. 29 Werkgroep 2005c
Art. 29 Werkgroep, Advies 5/2005 over het gebruik van locatiegegevens voor het verstrekken van diensten met toegevoegde waarde, WP115, 25 november 2005

Art. 29 Werkgroep 2006a
Art. 29 Werkgroep, Werkprogramma 2006-2007, WP120, 5 april 2006.

Art. 29 Werkgroep 2006b
Art. 29 Werkgroep, Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States (WP122), 14 juni 2006.

Nationale Ombudsman

Nationale Ombudsman, rapport 2003/348, 13 oktober 2003 <www.nationaleombudsman.nl>.

Publicaties Cbp (incl. Registratiekamer)

2000

Registratiekamer Advies aan de Minister van SZW, 22 september 2000, z2000-0845 (Concept-wetsvoorstel SUWI en privacybescherming).

Registratiekamer Advies aan de Minister van SZW, 28 november 2000, z2000-1179 (Wetsvoorstel Invoeringswet SUWI en privacybescherming).

Registratiekamer Uitspraak 10 januari 2001, z2000-1218 (correctie persoonsgegevens overledene).

Registratiekamer Uitspraak 20 juni 2001, z2000-0926 (medische dossiers op het internet).

2001

Registratiekamer Nader advies aan aan de Minister van SZW, 1 augustus 2001, z2001-0762 (conceptbesluit Inlichtingenbureau en SUWI).

Cbp Uitspraak 29 oktober 2001, z2001-0503 (gebruik kentekens voor identificatie van prostituanten).

2002

Cbp Uitspraak 14 januari 2002, z2001-1575 (Informatiehuishouding Bureau Jeugdzorg).

Cbp Advies aan de minister van SZW, 12 juni 2002, z2001-0267 (gegevensverkeer bij reïntegratie).

Cbp Advies aan de Minister van OCW, 7 november 2002, z2002-0964 (gebruik persoonsgebonden nummers in het voortgezet onderwijs).

Cbp Advies aan Burgermeester van Rotterdam, 27 november 2002, z2002-1335 (verstrekking historische strafrechtelijke gegevens aan samenwerkingsverbanden).

Cbp Onderzoeksrapport Onrechtmatig, onbehoorlijk en onzorgvuldig, april 2003

2003

Cbp Advies aan Minister SZW , 21 januari 2003, z2002-1512 (conceptbesluit tot wijziging besluit SUWI))

Cbp Uitspraak 4 februari 2003, z2002-1511 (vaststellen identiteit bij inzageverzoek).

Cbp Uitspraak 27 februari 2003, z2002-0831 (controlebevoegdheid zorgverzekeraar).

Cbp Uitspraak 4 maart 2003, z2002-0230 (inhuur verzekeringsgeneeskundigen).

Cbp, Advies aan de Minister van OCW, 22 april 2003, z2003-0284 (IQ-gegevens bijzondere gegevens).

Cbp Uitspraak 9 mei 2003, z2002-1085 (mailing apotheek).

Cbp Mededeling 26 juni 2003.

Cbp Verslag van de Expertmeeting Internationaal gegevensverkeer 1 juli 2003.

Cbp Advies aan de Minister van SZW, 1 september 2003, z2003-0872 (Wet financiering sociale verzekeringen).

Cbp Persbericht Contactdag gemeente FG's succesvol, 15 september 2003.

2004

Cbp Uitspraak 6 februari 2004, z2004-0165 (toezichtbevoegdheden Commissie toezicht OCW-veld).

Cbp Advies aan Staatssecretaris SZW, 30 maart 2004, z2004-0058 (aanpassing Circulaire gegevensuitwisseling SVB – gemeenten).

Cbp Uitspraak 13 mei 2004, z2004-0045 (verstrekking medische gegevens UWV).

Cbp Advies aan Ministerie van VWS, 27 juli 2004, z2004-0574 (Besluit beleidsinformatie jeugdzorg).

Cbp Uitspraak 8 september 2004, z2004-0724 (informeren autobezitters).

Cbp Advies aan Dagelijks Bestuur GGD, 4 oktober 2004, z2004-0583 (registratie vangnet).

Cbp Advies aan Minister van OCW, 12 november 2004, z2004-1182 (Besluit informatievoorziening WPO/WEC).

Cbp Brief aan Minister van Justitie, 7 december 2004, z2004-1086 (10 voorstellen voor reductie administratieve lasten WBP).

Cbp Jaarverslag 2004

2005

Cbp Advies aan Minister van Bestuurlijke Vernieuwing en Koninkrijkrelaties, 10 februari 2005, z2004-1734 (Wetsvoorstel burgerservicenummer).

Cbp Advies aan Staatssecretaris van Financiën, 16 maart 2005, z2005-0126 (Wetsvoorstel maatschappelijke ondersteuning).

Cbp Rapport Landelijke zorgregistraties, maart 2005

Cbp Advies aan Minister van VWS, 13 april 2005, z2005-0070 (Wet marktordening gezondheidszorg).

Cbp Mededeling Symposium 'Privacy in samenwerkingsverbanden', 24 mei 2005.

Cbp Uitspraak 27 mei 2005, z2004-1152 (informeren ouders door scholen).

Cbp Informatieblad Informatie delen in samenwerkingsverbanden, mei 2005.

Cbp Uitspraak 6 juni 2005, z2005-0355 (DBC-informatiesysteem).

Cbp Uitspraak 8 juni 2005, z2004-0742 (gebruik informatie over zwangerschap).

Cbp Advies aan Minister van OCW, 11 juli 2005, z2005-0502 (Pilot IBG-route).

Cbp Brief aan Minister van Justitie 12 juli 2005, z2004-1494 (Voorstellen wijziging Wbp).

Cbp Uitspraak 21 juli 2005, z2005-0505 (NICTIZ).

Cbp Uitspraak 11 oktober 2005, z2005-0878 (Landelijk Schakelpunt).

Cbp Advies aan de leden van de Vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties 25 oktober 2005, z2005-1198 (Burger Service Nummer).

Cbp Wetgever dient risico's van BSN aanzienlijk beter te ondervangen, 31 oktober 2005.

Cbp Reïntegratie van zieke werknemers en privacy, oktober 2005.

Cbp Uitspraak 1 december 2005, z2005-0212 (digitaal bouwarchief).

Cbp Rapport Landelijke zorgregistraties, 2005.

2006

Cbp Uitspraak 23 februari 2006, z2006-0238 (gebruik sofinummer door huisartsen).

Cbp Advies aan Minister van OCW, 14 maart 2006, z2006-0154 (Ontwerpbesluit houdende wijziging van het Formatiebesluit WPO ivm wijziging gewichtenregeling).

Cbp Uitspraak 9 mei 2006, z2005-1372 (Online afsprakensysteem Flevoziekenhuis).

Cbp Publicatie van persoonsgegevens op internet, 17 mei 2006.

Cbp Particuliere recherche en bescherming van persoonsgegevens, 23 mei 2006.

Cbp Nieuwsbericht 'Cbp roept op tot naleven meldingsplicht', 21 januari 2003.

Kamerstukken

Wetvoorstel persoonsregistraties, *Kamerstukken II* 1986/1987, 19095, nrs. 6-23

Rijksbegroting Justitie 1993, *Kamerstukken II* 1992/1993, 22 800 VI, nr. 43.

Rijksbegroting Justitie 1995, *Kamerstukken II* 1994/1995, 23 900 VI, nr.13 .

Wetsvoorstel bescherming persoonsgegevens *Kamerstukken II* 1997/98-1999/2000, 25 892, nrs. 1-35; *Kamerstukken I* 1999/2000, 25892, nrs 92-92e

Wijziging bepalingen m.b.t. de verwerking van persoonsgegevens, *Kamerstukken-II* 1998/99-2000/01, 26410, nrs. 1-10; *Kamerstukken I* 2000/2001, 26 410, nrs. 150-150c

Kaderstellende visie op toezicht *Kamerstukken* II 2000-2001, 27 831, nr. 1.

Wet openbaarmaking uit publieke middelen gefinancierde topinkomens *Kamerstukken II* 2004-2005, 30 189, nr. 3.

Vaststelling begroting van het Ministerie van Justitie 2005 *Kamerstukken II* 2005-2006, 29 800, nr. 163.

Wet algemene bepalingen burgerservicenummer *Kamerstukken II* 2005-2006, 30 312, nrs. 1-9.

Jaarverslagen FG

Jaarverslag FG Ministerie van VROM 2003.

Jaarverslag FG Gemeente Arnhem 2005.

Jaarverslag FG Gemeente Best 2005.

Jaarverslag FG Inlichtingenbureau 2005.

Jaarverslag FG Ministerie van EZ 2003.

Jaarverslag FG Ministerie van LNV 2003/2004.

Jaarverslag FG Ministerie van VROM 2003 & 2004.

Jaarverslag FG Ministerie van VWS 2003.

Bijlagen

Bijlage A. Bij het onderzoek betrokken personen

Projectleiding:

Gerrit-Jan Zwenne - eLaw@Leiden

Onderzoekers:

Gerrit-Jan Zwenne, Hugo Kielman, Wouter Koelewijn en Laurens Mommers - eLaw@Leiden

Marga Groothuis - Afdeling Staats- en bestuursrecht, Universiteit Leiden

Anne-Wil Duthler - Duthler Associates

Onderzoeksassistentie:

Peter van Schijndel - eLaw@Leiden

Jean Paul van Schoonhoven - Duthler Associates

Expertbijeenkomst 23 augustus 2006

Dr. P.W.J. de Graaf - VNO-NCW

Mw. drs. M.A.M. Lenssen - Gemeente Horst aan de Maas

Mr. J. de Zeeuw - Ministerie LNV

Mr. W. Simonis - Ministerie BuZa

Drs. M.C. Romijn - HS Utrecht

Drs. R.J. Hageman - Nationaal Archief

Mw. drs. K. de Jonge - Consumentenbond

Dhr. A.A.M. Jean Pierre - IB-groep

Mr. drs. J. van Leeuwen - TU Delft

Mr. H. Gardeniers - Net2Legal

Mr. J.P.R. Bergfeld - Inlichtingen Bureau

Dhr. M. Kahr - Intrum Justitia

Drs. J.C. Buitelaar - Ministerie OCW en Ministerie SZW / NGFG

Mw. mr. Z. Titulaer - NGFG

Mr. A.J.J.T. Singewald - op persoonlijke titel

High-level expertbijeenkomst 29 augustus 2006

Prof. dr. P.J.A. (Paul) de Hert

Mr. A. (Alexander) Patijn

Prof. mr. G. (Margriet) Overkleeft-Verburg

Mr. H. (Hester) de Vries

Interviews gehouden door H.H. Kielman en W.I. Koelewijn

Mr. drs. J.H.J. Terstegge - Philips International B.V. (3 augustus 2006)

Dr. J. Holvast - Holvast & Partner (2 augustus 2006)

A. Schuiteman - Sociale Verzekeringsbank

Mr. W.A. Sinninghe Damsté - Sociale Verzekeringsbank (16 augustus 2006)

Bijlage B. Summary

This report concerns the first evaluation phase of the Dutch Data Protection Act (*Wet bescherming persoonsgegevens* hereinafter 'DPA' or 'the act'), as referred to in section 80 DPA. First, an inventory has been made of the objectives stated upon the introduction of the DPA. In addition – to the extent to which these objectives are related to the implementation of privacy directive 95/46/EC – it was checked what the intentions of the community legislator were (inventory of the objectives). Subsequently, it has been investigated which obstacles were observed in literature and case law upon the implementation and application of the act (obstacle analysis). The purpose of this investigation is to make recommendations for the further formulation of research questions for the second evaluation phase (formulation of questions).

The DPA consists in the implementation of privacy directive 95/46/EC in the Dutch legal system. This is why the first part of the objective inventory covers the intentions of the community legislator (chapter 2). Through this directive, the community legislator intends to contribute to the realization of the general objectives of the community. It does so by contributing to the realization and operation of the internal market on the one hand and by providing warranties for the protection of fundamental rights and freedoms on the other hand. The contribution to the internal market is vested in the removal of internal market barriers that may arise from the differences between national statutory regimes for the processing of personal data. This is why the community legislator opted for a broad application scope for the directive that particularly, but not exclusively, concerns automated processing. To guarantee fundamental rights and freedoms, the directive intends to reach an equal and high level of protection for all member states through harmonization of laws. In connection with the realization of a high level of protection, the directive refers to the European Convention on Human Rights and Fundamental Freedoms (ECHR) and the privacy principles that have been laid down in the Council of Europe's Convention 108 on the protection of individuals with regard to automated processing of personal data (Convention on data protection). Furthermore, the high level of protection must be reached by improving the transparency of data processing and by providing warranties for the persons involved. In order to reach an equal level of protection, the directive intends to harmonize the national privacy acts of member states, and to provide that in different member states similar arrangements and obligations apply to the protection of personal data.

Finally, the community legislator also wanted to meet the peculiarities of certain categories of data or processing. This is why he provides 'a certain bandwidth' to the national legislator in particular cases. That flexibility is also expressed in the objective to take as much as possible account of the specific circumstances and needs of a sector or line of business. Therefore, the directive provides the option that codes of conduct are drawn up at the level of the sector or line of business.

The second part of the inventory of the objectives covers the intentions of the national legislator with the introduction of the DPA (chapter 3). A distinction was made between the procedural and substantive objectives of the DPA. The procedural objectives arise from the obligations to which the legislator is bound pursuant to higher laws such as the EC Treaty and the privacy directive. The substantive objectives concern the ways in which the procedural objectives have been realized.

The first procedural objective of the DPA is the implementation of the directive and the further materalization of the conditions under which processing is lawful. It is the intention of the national legislator that a further realization of the standards from the DPA must take place in sectoral legislation and self-regulation, and in case law. The second procedural objective concerns the implementation of the instruction by the constitutional legislator to lay down rules in connection with the recording and provision of personal data. Finally, the third procedural objective is the implementation of the Convention on data protection and the connection to the relevant case law of the European Court of Human Rights.

With respect to the substantive objectives, the DPA first intends to provide warranties that provide a balance between privacy protection and other fundamental rights. The legislator opted for using open stan-

dards, because through this, a set of instruments is provided by means of which the interests involved in the data processing can always be weighed. In that respect, it is of interest to the legislator that the DPA is well embedded in the legal system and links up with existing case law.

Furthermore, the DPA concerns the reinforcement of the controllers' position by clarifying the controller concept and by increasing the transparency of the data processing. For this, the act grants rights to the persons involved and imposes corresponding obligations on controllers. For the supervision and monitoring of the compliance with the act, the Dutch Data Protection Authority (*College bescherming persoonsgegevens* hereinafter 'the Authority') has been set up. In addition to this central regulatory authority, the act also provides the option to appoint a Data Protection Officer (DPO). The object of this is to promote the development of knowledge on data protection and privacy awareness in controllers. The notification obligation can also be regarded as a way of stimulating self-regulation at the controller level.

In the inventory of the obstacles, first the most striking general obstacles with respect to the application and implementation of the DPA have been mapped on the basis of literature study (chapter 4). Some authors first see the lack of clarity and vagueness of the statutory concepts as obstacles, because they impede the compliance with the law and may obstruct technological development and innovation. Other authors on the contrary plead for the preservation of the broad application scope.

In literature, reference is further made to obstacles arising from the general, comprehensive character of the act. These particularly concern the complexity and inflexibility of the act. On the other hand, some other authors think that this comprehensive aspect is necessary in order to regard all interests involved in their cohesion. It turned out that the domain experts consulted in the scope of this investigation had little support for a sectoral approach instead of the current all comprising approach.

In addition, in literature, obstacles have been observed concerning the determination of which person is the controller to whom the substantive standards of the law are primarily applicable. These problems especially occur in joint venture constructions, and in the context of the internet. According to some authors, the act has a unilateral procedural character and does not provide sufficiently firm substantive standards. According to other authors, the act is too unpractical because it assumes that each processing is tested against the (too vague) standards of the DPA. They also criticize the designation of a whole category of data as special data. In practice, this leads to obstacles because the sensitivity of special data depends on the context.

With respect to the realization of codes of conduct, some authors regard the influence which the DPA has pursuant to its approving power as an obstacle. According to them, drafting codes of conduct is a long-term, time-consuming and expensive process which does not have many concrete advantages. Literature also has doubts about guaranteeing the independence of the DPO. The professional association for DPO's insists upon more DPO's being appointed in the private sector. Also with regard to the DPO's contribution to increasing the transparency of processing, the opinions vary. In literature, a discussion has arisen on the question whether the Authority has sufficient or insufficient powers. The obstacles with respect to the compliance with the act and obstacles in the field of enforcement are emphasized. In this line, critical comments are also made on the system of legal protection. Drawbacks are connected to the multiple administrative and civil law proceedings, such as forum shopping. The multiple legal competences may also affect the unity of law.

With respect to the international transfer of personal data, especially the permit requirement is experienced as an obstacle. This particularly applies to the transfer of personal data from an office of a controller within the EU to an office of the controller beyond the EU. This 'internal' transfer does not fall under the exceptions to the transfer prohibition. Arguments are also advanced for decreasing the compliance cost for controllers through the abolishment of the license obligation when model contracts destined for that purpose are used.

In the private sector (chapter 5), with respect to the conceptual framework of the DPA obstacles are mainly found in multinationals. Particularly the obscurities and vagueness of important concepts, such as personal data, processing, controller and processor, give rise to problems in international data streams, mergers and acquisitions. Further obstacles are observed with respect to the connection of the DPA to other legislation, like the Database Act (*Databankenwet*) and the Act Electronic Commerce Directive (*Aanpassingswet inzake richtlijn elektronische handel*). A difference in the use of the concepts leads to confusion there. Other application problems are related to the formulation of the prescriptive framework of the DPA. In the private sector, this results therein that the DPA does not give a clear picture in all cases of what is allowed and what is not. Literature shows in any case that there are obstacles in the private sector with regard to the concept of 'consent' and 'justified interest', and the (un)lawful access to (special) data by third parties.

An important objective of the DPA concerns the transparency and reinforcement of the position of the persons involved. From literature, the picture arises that there are obstacles in the private sector regarding the notification of personal data processing and the impossibility to use the exemption from the notification obligation included in the Exemption Decree (*Vrijstellingsbesluit*). These comments concern the electronic notification system that is categorized as inconvenient; the inefficacy of the exemption decree due to the many details, and a compulsory public access of the data in the notification system as a direct consequence of the notification. Furthermore, literature shows that there are obstacles in the design of and compliance with the obligation to provide information. Informing the persons involved beforehand is labour-intensive and sometimes clashes with the confidential character of the data processing in question. In addition, the obligation to provide information is considered to be hard to apply through the use of open standards. With respect to the rights of the persons involved, there are obscurities in the scope of the right to information.

An interested party may appeal against certain decisions of the controller with the district court. In literature, a number of obstacles are observed with regard to this 'new' legal action. The unfamiliarity of judges with the DPA and the ambiguity and high threshold of civil proceedings are pointed to. The checking of and supervision over data processing in the private sector initially are the responsibility of the DPA. This Authority seems to be inclined to make use of an active publication policy within the scope of its supervisory responsibilities ('naming and shaming').

With respect to the public sector (chapter 6), literature shows obstacles similar to those found in the private sector. In the public sector there are also obscurities on the interpretation and application of concepts like controller and personal data, and on the relationship between the DPA and other acts, such as the Government Information Public Access Act (*Wet openbaarheid van bestuur*) and the Public Administration Probity in Decision-making Act (*Wet bevordering integere besluitvorming openbaar bestuur*). Especially, the presence of many sectoral rules on the use of personal data, such as Municipal Database Personal Files Act (*Wet gemeentelijke basisadministratie persoonsgegevens*), Police Files Act (*Wet politieregisters*), is typical for the public sector. This restricts the DPA's application scope in this sector.

With respect to the material norms in the Act obstacles arise in the public sector particularly with regard to the prohibition of the processing of special data. This particularly applies to the monitoring of the compliance with legislation for which special data like health data are kept. Further, with respect to the theme of self-regulation it is striking that in the public sector relatively many DPO's have been appointed, but that no codes of conduct exist. An informal way of self-regulation does exist, such as networks or platforms within which arrangements are made on data processing or best practices are exchanged for example.

In the public sector the inspection and correction rights do not seem to be very common. There are indications that procedures and measures are missing for enabling the implementation of these rights in a careful way within the statutory term.

With respect to the subject supervision and legal protection, a number of specific obstacles have been observed in the public sector. The processing time of the preceding investigation, which is carried out compulsorily in some cases by the DPA, may constitute an obstacle, particularly for collaborative projects. The exercise of the supervision by PDO's barely creates obstacles in the public sector. This does not apply to legal protection, which has been regulated differently in the public sector than in the private sector. According to some authors, this is detrimental to the unity of law and the privacy protection.

In the semi-public sector (chapter 7), some of the act's core concepts also lead to problems. For example, the vagueness of the concept of personal data implies obscurity on the scope of the act and this leads to divergent interpretations. The concepts of controller and processor are regarded as unclear. It is also indicated that the application of the DPA in the semi-public sector is impeded by a multitude of sectoral regulations. In combination with the high abstraction of the DPA, this leads to an incomprehensible system of rules. In addition, in practice the DPA is considered as impeding the effectiveness of policy in which a 'customer-friendly' service provision is aimed at, by asking citizens' data only once. In connection with this, literature shows that social workers in collaborative projects and 'chain care' (*ketenzorg*) are unaware of the interpretation space of the DPA. In some cases, this unfamiliarity results in social workers erroneously assuming that particular forms of data processing are not allowed. The prescriptive frameworks of the DPA raise some specific questions in the semi-public sector, for example in the social service and health care sector. Where acts are performed without the consent of the person involved, the DPA raises impediments.

With respect to the theme of self-regulation it appears that the code of conduct that is applicable to health care insurers increases the density of rules, but is not sufficiently able to react adequately to new developments within the social service sector. With respect to the transparency objective and the rights of the persons involved, similar obstacles are observed in the semi-public sector as in the other sectors. The implementation of the inspection right for both the person involved and the controller is impeded by a number of practical problems that are regarded as a consequence of the high abstraction level and the too rigid standard in the so-called Costs Decree (*Vrijstellingsbesluit*). Furthermore, there are signs that the obligation to provide information and the requirement of consent result in relatively high effecting costs for large implementing organizations.

In case law and literature, little obstacles are observed that specifically refer to the legal protection, enforcement and supervision within the semi-public sector. The various pieces of legislative advice and decisions by the DPA raise the impression that the supervision over, and the enforcement of the law have been regulated properly. In this respect, the danger of pseudo-legislation is pointed to. With respect to legal protection, the unfamiliarity with and the interrelated false application of the opposition right form the most striking obstacles.

Finally, on the basis of the inventory of the obstacles it has been checked to which extent the objectives of the DPA and, if relevant, of the directive have been made (chapter 8). For this, the different obstacles which were found in literature were linked to the objectives of the Dutch legislator. Subsequently, the most important conclusions were regarded from three evaluation perspectives.

First, the legal perspective points to the most important obstacles arising from the difficult connection of the DPA with the Dutch legal system. The layered and compartmented system for the protection of personal data has become very complex and sometimes tends to overregulation. In addition, the conceptual system and set of instruments of the DPA as such are too abstract and leave too much space for interpretation to form a clear framework for the assessment of concrete questions and situations. With this, the objective of the determination of a conceptual system that can be used for legal formation and for the weighing of interests is not fully realized.

Secondly, from the perspective of enforcement and compliance the unilateral character of the enforcement can be pointed to, as the emphasis mainly lies on the usually followed administrative law process. In

addition, the intended system of checks and balances is only shaped to a restricted extent by the lack of factual legal review of the principles from the DPA. Furthermore, self-regulation within the scope of the DPA leaves much to be desired. It can also be concluded that particularly the objectives of the legal review of the powers granted to the Authority and the further interpretation of substantive standards through self-regulation have only been realized to a restricted extent.

Thirdly, from the perspective of awareness and familiarity, it is striking that many rights and obligations of controllers and persons involved that arise from the DPA are not effectively exercised through a lack of familiarity with these rights and obligations. One of the central objectives of the DPA, i.e. increasing the transparency of data processing through the granting of rights and obligations and the introduction of a regulatory authority seem to have been (partially) unrealized. Finally, the overview from the three perspectives constitutes the starting point for the determination of relevant questions for the second phase of the evaluation in which the effectiveness of the DPA will be researched empirically.