

Scheiding der machten bij of krachtens de WBP

238

Trefwoorden:

Evaluatie WBP, zelfregulering, machtscheiding

De evaluatie van de Wet bescherming persoonsgegevens is aanstaande. Met de evaluatie zal verslag worden gegeven over de doeltreffendheid en de effecten van de Wet bescherming persoonsgegevens in de praktijk. Een bijzonder aandachtspunt bij de evaluatie is de beoordeling of het huidige beschermingsniveau als gevolg van technologische ontwikkelingen behouden blijft. De Wet bescherming persoonsgegevens gaat uit van een zo technologieonafhankelijk mogelijke benadering. Gedragsvoorschriften in wet- en regelgeving worden niet wenselijk geacht. Zelfregulering is dus wenselijk en passend. Daarnaast levert zelfregulering een positieve bijdrage aan de oorspronkelijke gedachte van scheiding der machten binnen de Nederlandse rechtsstaat.

1 Inleiding

Het verband tussen trias politica, ICT en gegevensbescherming lijkt vergezocht. Zo is de trias politica een uitwerking van de idee van scheiding der machten binnen een staat. Het is een politiek systeem dat meestal in verband wordt gebracht met de Fransman Charles Montesquieu. ICT en gegevensbescherming zijn geen machten binnen een staat noch brengen ze op enigerlei wijze een rangorde of differentiatie aan. Welke gevolgen of invloed hebben ICT-ontwikkelingen op gegevensbescherming en wat is dan de invloed daarvan op het beginsel van machtscheiding?

Deze vraag wordt in dit artikel beantwoord. Ik maak daarbij een onderscheid in 'trias-gedachten'. Vooropstaat de klassieke gedachte. Deze gedachte gaat uit van de scheiding der machten op staatsniveau, te weten de wetgevende macht, de uitvoerende macht en de rechtsprekende macht. Daarnaast onderscheid ik ten behoeve van dit artikel, binnen een van de klassieke machten, een verdeling naar regelgevende, uitvoerende en toezichhoudende organisaties. Verder onderscheid ik binnen een organisatie een verdeling naar beleidsbepalende, uitvoerende en controlerende functies.

2 Evaluatie WBP

2.1 Art. 80 WBP

Art. 80 WBP bepaalt dat de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties binnen vijf jaren

na de inwerkingtreding van de WBP aan de Staten-Generaal een verslag zenden over de doeltreffendheid en de effecten van de WBP in de praktijk. De memorie van toelichting bij dit artikel voegt daar nog met zoveel woorden aan toe dat het gelet op de snelle informatietechnologische ontwikkelingen dienstig is een evaluatiebepaling op te nemen om te bezien of bepalingen van de WBP wellicht knelpunten opleveren, dan wel de bescherming van de persoonlijke levenssfeer ontoereikend garanderen. De WBP is in werking getreden op 1 september 2001 en het evaluatieverslag zou dus voor 1 september 2006 aan de Staten-Generaal moeten zijn gezonden. Het ministerie van Justitie heeft er echter voor gekozen de evaluatie uit te stellen en in twee fasen te verdelen. Fase 1 omvat een literatuur- en jurisprudentieonderzoek en zal naar verwachting dit najaar gereed zijn. Fase 2 zal een juridisch en een sociaalwetenschappelijk deel bevatten en komt gereed in de loop van 2007.

De tenuitvoerlegging van de WBP valt, vanuit de klassieke gedachte van de trias geredeneerd, onder de uitvoerende macht. Eventuele conclusies van de evaluatie van de WBP kunnen evenwel ook gevolgen hebben voor de beide andere machten. Als de WBP zou moeten worden aangepast, dient dit door de wetgevende macht te gebeuren (regering en Staten-Generaal tezamen). Een wijziging van de wet heeft daarnaast ook invloed op de rechterlijke macht. Zij is het immers die de uitvoering van wetten en regelgeving controleert.

De bondigheid van de evaluatieopdracht in art. 80 WBP is omgekeerd evenredig aan de complexiteit van de uitvoering. De wetgever gaf bij het wetsvoorstel WBP al aan dat een sluitend systeem van regels over de verwerking van persoonsgegevens wel nooit mogelijk zal zijn en in ieder geval gegeven de snelle technologische ontwikkelingen (lees hier: ICT) niet wenselijk. Verder gaf de wetgever aan dat 'het recht op bescherming van persoonsgegevens in de aanzwellende informatiemaatschappij een zich geleidelijk ontwikkelende dogmatiek voor een nieuw rechtsgebied vergt dat nog maar in de kinderschoenen staat.' Ook gaf de wetgever aan dat 'de technologische ontwikkelingen daarmee het recht voor uitdagingen stellen die slechts door de geleidelijke ontwikkeling van nieuwe rechtsbegrippen en daarmee verbonden rechten het hoofd kunnen worden geboden. Een uitgekristalliseerd juridisch begrippenapparaat en een vaststaande invulling daarvan in de juridische dogmatiek, zal pas beschikbaar zijn wanneer ook de informatietechnologische ontwikkelingen in een rustiger vaarwater zijn gekomen.'¹

De WBP vormt de Nederlandse implementatie van de Richtlijn nr. 95/46/EG. Een van de uitgangspunten van de richtlijn die in de WBP is overgenomen, betreft het streven

* Jean Paul van Schoonhoven is als adviseur ICT en Recht werkzaam bij Duthler Associates in Den Haag. Daarvoor werkte hij als beleidsmedewerker bij het CBP. Citeertitel: J.P. van Schoonhoven,

'Scheiding der machten bij of krachtens de WBP', *P&I* 2006, 238.

1 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 40 (MvT).

naar zo technologieonafhankelijk mogelijke wetgeving (volledig technologieonafhankelijke wetgeving is niet reëel). Vanuit een juridische blik bezien brengt dit echter (rechts)onzekerheid met zich mee. De wetgever signaleert dit in de memorie van toelichting bij de WBP door te schrijven dat om greep te kunnen houden op mogelijke bedreigingen voor de menselijke waardigheid,² een wet zo helder en duidelijk mogelijk moet zijn. Het moet de gedragsvoorschriften³ geven voor een nieuwe technologie. Alleen, meestal is onduidelijk hoe nieuwe technologieën zich ontwikkelen. De wetgever tast dan in het duister over de te geven gedragsvoorschriften.⁴

Bij de lezer van dit artikel zou de gedachte kunnen opkomen dat de evaluatie van de WBP geen sinecure is. De WBP moet namelijk geëvalueerd worden om te bezien of hij tegen de achtergrond van de technologische ontwikkelingen knelpunten oplevert die moeten worden opgelost. Hiertoe zal allereerst in kaart moeten worden gebracht welke technologische ontwikkelingen er zijn en of deze knelpunten opleveren. Daarna zal voor iedere ontwikkeling die een knelpunt oplevert, beoordeeld moeten worden of de ontwikkeling al voldoende in rustiger vaarwater is gekomen en of er een uitgekristalliseerd juridisch begrippenapparaat beschikbaar is. Vervolgens zal moeten worden beoordeeld of dat begrippenapparaat zich ook leent voor normering door middel van opname in de WBP. Tegelijkertijd moet bij het wettechnisch oplossen van een knelpunt, de WBP zo technologieonafhankelijk mogelijk blijven, maar ook weer helder genoeg zijn om normen te geven. Normen die de 'menselijke waardigheid' (lees hier: bescherming van onze persoonsgegevens) beschermen tegen mogelijke bedreigingen.

Betekent dit nu dat bij geconstateerde knelpunten rustig moet worden afgewacht tot technologische ontwikkelingen voldoende helder en uitgemaakt zijn en dat geaccepteerd moet worden dat rechtsonzekerheid tot die tijd blijft bestaan? Geenzins. 'De vruchten van nieuwe technologische mogelijkheden moeten worden verenigd met een nieuwe verantwoordelijkheid van de mens om zodanig met informatie om te gaan, dat een humane informatiemaatschappij als nieuw cultuurgoed wordt verwerkelijk. Dit noopt tot de ontwikkeling van nieuwe normen en waarden die voor een deel ook in het recht moeten worden vastgelegd.⁵ Anders gezegd: de onduidelijkheid van wetgeving ter bescherming van persoonsgegevens komt vaak voort uit de veronderstelling dat deze wetgeving volledige (specifieke) gedragsvoorschriften bevat. Ook komt onduidelijkheid vaak voort uit de veronderstelling dat wetgeving verantwoordelijken zonder meer duidelijkheid verschaft. Deze veronderstellingen zijn onjuist. Op iedere verantwoor-

delijke rust de zelfstandige plicht tot inachtneming van de beginselen van behoorlijk bestuur (in de publieke sector) of van de maatschappelijke zorgvuldigheid (in de private sector). Dit ongeacht het voorhanden zijn van een specifiek gedragsvoorschrift. Ook is het zo dat wetgeving nooit volledig kán zijn.

Zelfregulering kan dientengevolge een rol spelen bij het toepassen van de (geest van de) wet. Dit vergroot tevens de rechtszekerheid.

2.2 Technologische ontwikkelingen

De gegevens van een burger staan in honderden bestanden. Door technologische ontwikkelingen wordt het opslaan van gegevens steeds gemakkelijker en worden de gegevensbestanden alsmede de mogelijkheden tot koppeling van bestanden, al dan niet via het internet, steeds groter. Nieuwe ontwikkelingen zijn vaak complex en niet of nauwelijks inzichtelijk voor de burger. Daarmee zijn ook zijn mogelijkheden tot controle beperkt. Tegelijkertijd bieden de ontwikkelingen ook kansen. Niet alleen vanuit het gebruikersgemak, maar ook vanuit het oogpunt van kenbaarheid. Zo kunnen burgers sneller, gemakkelijker en beter worden geïnformeerd door de toenemende mogelijkheden van elektronische communicatie. De angst die nog maar enkele decennia geleden bestond voor gegevensverzameling in computerbestanden,⁶ is voor veel mensen geen realiteit geworden. Percepties en maatschappelijke acceptaties ten aanzien van technologie kunnen veranderen en angst kan overgaan in vertrouwen en geloof in techniek. Een voorbeeld hiervan is de grote vlucht die het internet heeft genomen (weblogs, nieuwsgroepen, onlinewinkels, msn (online chatten), hyves (onlinevriendennetwerk), enz.) en het vertrouwen dat gebruikers hierin stellen. Een ander voorbeeld is het intensieve gebruik van mobiele telefoons. Midden jaren negentig was het al heel wat om een mobieltje te hebben en dan nog werd dit vaak gebruikt 'voor noodgevallen'. Anno 2006 ligt het mobieltje op ons nachtkastje en worden we ongerust als we iemand niet direct te spreken krijgen, we kijken er tv op, internetten, chatten, sms'en ermee en maken foto's en video's zo veel en zo vaak als we willen.

Een aantal technologische ontwikkelingen die een hoge vlucht hebben genomen sinds de inwerkingtreding van de Europese richtlijn en de WBP betreffen:

- het internet;
- de toepassing van biometrie (denk aan de irisscan op Schiphol, het nieuwe paspoort, de vingerafdrukken als u naar of via de Verenigde Staten reist of de inzet van intelligente camera's in stadions of in de openbare ruimte);

2 Zie over het gebruik van de term 'menselijke waardigheid' onder meer (eerder aangehaalde gedeelten uit) de memorie van toelichting bij de WBP en een uitspraak van het Duitse Constitutionele Hof van 15 december 1983.

3 Voorbeelden van gedragsvoorschriften van de WBP zijn de eisen van een zorgvuldige, transparante en proportionele gegevensverwerking.

4 Kamerstukken II 1997/98, 25 892, nr. 3, p. 41 (MvT).

5 Kamerstukken II 1997/98, 25 892, nr. 3, p. 3 (MvT).

6 Bij de laatste volkstelling van 1971 brak landelijk rumoer uit en werd de roep om privacybescherming steeds luider. Proeftellingen voor de geplande volkstelling van 1981 lieten een onverwachts hoge non-respons van 26% zien. Zie bijvoorbeeld het artikel van D. Pinedo, 'Mooi zo, de dinosaurus is dood', *NRC Handelsblad* 7 januari 1999.

- RFID⁷ (denk aan de onderhuidse implementatie van een RFID tag ter voldoening van uw drankrekening bij de Baja Beach club, het beveiligen van goederen tegen winkeldiefstal, het traceren van goederen in een logistieke keten);
- spyware (software die ongevraagd en ongewenst al dan niet wordt geïnstalleerd op uw computer om bepaalde gegevens te achterhalen);
- cookies (kleine tekstbestanden die op uw computer worden weggeschreven zodat u bijvoorbeeld bij een volgend bezoek aan een website wordt herkend);
- e-maildiensten (denk aan Gmail van Google dat automatisch de inhoud van uw e-mails scant om u daaraan gerelateerde reclame te kunnen sturen);
- de opslag van (verkeers)gegevens van telecommunicatie (bijvoorbeeld ten behoeve van terrorismebestrijding door de overheid, maar ook voor het door een provider kunnen versturen van de rekening voor aan u geleverde communicatiediensten, zoals telefonie of internet);
- de Diagnose Behandel Combinaties in de zorg; of
- de voorgenomen invoering van de ov-chipcard.

Deze ontwikkelingen bestonden grotendeels al op het moment dat de regelgeving werd aangenomen, maar waren toen allesbehalve uitgekristalliseerd en specifieke gedragsvoorschriften zijn dan ook nog niet door de wetgever geformuleerd. Een veelgehoorde vraag in dat verband bij burgers en verantwoordelijken is waarom de wetgever dan niet heeft gewacht met de invoering van regelgeving ter bescherming van de persoonsgegevens? Om die vraag te kunnen beantwoorden is het nodig hieronder een kort uitstapje te maken naar de historie van de WBP.

2.3 Historie WBP

Het grondbeginsel van het recht op privacy is vastgelegd in art. 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) uit 1950. Teneinde vervolgens aan de gegroeide behoefte aan normering van het gebruik van persoonsgegevens te voldoen, wordt in 1981 het Verdrag van Straatsburg aangenomen. In Nederland is tegelijkertijd de Commissie-Koopmans bezig een rapport op te stellen voor de herziening van de Grondwet. In het eindrapport van de commissie wordt geconcludeerd: '(...) de eerbiediging van de persoonlijke levenssfeer wordt in onze samenleving thans terecht beschouwd als een essentiële voorwaarde voor een menswaardig bestaan en als een van de grondslagen van onze rechtsorde.' De bescherming van de persoonlijke levenssfeer wordt opgenomen in art. 10 van de Grondwet. In 2000 brengt de Commissie 'Grondrechten in het digitale tijdperk' een advies uit over onder meer aanpassing van art. 10 Grondwet met het oog op de ontwikkelingen op het terrein van ICT. Mede naar aanleiding van het advies van de Raad van State besluit het kabinet in 2004 de voorstellen tot wij-

ziging van de Grondwet in te trekken. Wel komen er nieuwe voorstellen, maar daarbij zullen de internationaalrechtelijke ontwikkelingen op het gebied van de toepassing van mensenrechten in de informatiesamenleving worden betrokken.

In navolging van de opdracht uit art. 10 Grondwet, trad op 1 juli 1989 de Wet persoonsregistraties (WPR) in werking. Vaststelling van de WPR was tevens voorwaarde voor toetreding tot het Verdrag van Straatsburg dat in 1993 werd geratificeerd. Met de WPR werd tegelijkertijd ook de uit art. 8 EVRM voortvloeiende positieve regelingsverplichting nagekomen. In 1995 komt de Richtlijn nr. 95/46/EG tot stand. Deze richtlijn is gebaseerd op het Verdrag van Straatsburg, maar geeft een nadere uitwerking aan het verdrag en voegt ook nieuwe elementen toe. Tot slot trad op 1 september 2001 de WBP in werking ter implementatie van de richtlijn.

De reden dat dan ook niet gewacht kon worden op de ontwikkelingen op het technologische vlak was dat men op Europees niveau al veertien jaar (mede als gevolg van de grote invloed van verscheidene krachtige lobby's) probeerde Europese regelgeving tot stand te brengen. Toen het dan ook eenmaal zover was, moest de Nederlandse wetgever wel tot implementatie overgaan, op straffe van een boete van de Europese Commissie. Uiteindelijk werd de WBP overigens toch nog te laat geïmplementeerd.

In ambtelijke kringen wordt over het voorgaande nog wel eens opgemerkt dat het 'twintig jaar duurde om te komen tot de WBP, maar uiteindelijk kwam die nog vijf jaar te vroeg'. In deze kreet zit zeker een kern van waarheid. De uitvoerende macht worstelt al geruime tijd met de toepassing van de WBP in concrete situaties waarbij bijvoorbeeld sprake is van complexe en dynamische computersystemen die zich niet of nauwelijks laten vangen door de rigiditeit van de wet. De verwerking van persoonsgegevens binnen een mondiaal opererend concern vormt hiervan een mooi voorbeeld. Op grond van de WBP dient een vergunning te worden gevraagd aan de Minister van Justitie voor het gebruik van bijvoorbeeld een *human resources systeem* binnen een concern, welk systeem draaiende wordt gehouden door een server buiten het grondgebied van de Europese Unie, ook al blijven de gegevens alleen beschikbaar voor de concernmaatschappij binnen de Europese Unie. Een ander fraai voorbeeld is dat (privé) websites door een uitspraak van het Europese Hof van Justitie (de zaak *Lindqvist*) onder de werking van de richtlijn vallen.

De komende wetsevaluatie, vijf jaren na de inwerking-treding van de WBP, kan dan ook een goede gelegenheid vormen eventuele gedragsvoorschriften voor de normering van (bepaalde) technologische ontwikkelingen te onderkennen, te formuleren en uiteindelijk in een gewijzigde WBP en/of andere wetten vast te leggen. De meningen hierover zijn evenwel verdeeld en ook zijn er alternatieven beschikbaar.

⁷ Radio Frequency Identification is een methode om van een afstand informatie op te slaan en te lezen van zogenaamde 'tags' die op of in objecten zitten.

2.4 Debat

In een essay van Prins⁸ is een achttal interviews opgenomen over verleden, heden en toekomst van gegevensbescherming. Uit de interviews komt onder meer naar voren dat er meer aandacht moet komen voor zelfregulering, dat het *controledenken* (dat wil zeggen gericht op beheersing van gegevensstromen door greep op de technologie) is achterhaald, dat er begrip moet worden getoond voor de sociale werkelijkheid waarin het recht functioneert en dat beleidsmakers, wetenschappers en burgers een meer kritische houding moeten aannemen ten opzichte van technologie.

Roßnagel en Müller⁹ geven in een artikel vier normatieve aanzetten die antwoord kunnen bieden op de onzekerheden die kunnen bestaan ten aanzien van de toepassing van gegevensbescherming op nieuwe technologische ontwikkelingen. Ten eerste maken zij een onderscheid tussen verwerkingen van persoonsgegevens met en zonder een gericht doel. Ten tweede stellen ze dat individuele controle op verwerkingen bijna niet meer mogelijk is waardoor controlebevoegdheden zouden moeten worden overgedragen aan personen of organisaties die het vertrouwen van de betrokkenen hebben. Deze controles moeten daarbij meer gericht zijn op de (structuren en functionaliteiten van) systemen en niet op individuele gegevensbescherming. Ten derde moet er rekening worden gehouden met de constante rolwisselingen tussen verantwoordelijken en betrokkenen, wie door de betrokkene moet worden aangesproken is steeds onduidelijker. Daarom moeten alle partijen die een rol spelen in ontwikkeling van technologie worden aangesproken. En ten vierde dienen er preventieve maatregelen te worden genomen bij het ontwerpen van systemen, dus ook vóór er sprake is van verwerking van persoonsgegevens.¹⁰

In het voorgaande is met name ingegaan op de aanstaande wetsevaluatie en technologische ontwikkelingen. ICT heeft echter ook onmiskenbaar invloed op de rol van de 'privacy' toezichthouder, het CBP. In de volgende paragraaf zal hierop nader worden ingegaan.

3 College bescherming persoonsgegevens

3.1 Viersporenbeleid en zelfregulering

Het CBP heeft ervoor gekozen de bescherming van persoonsgegevens langs vier sporen te bevorderen. Het eerste spoor heeft betrekking op bewustwording, het tweede spoor op normontwikkeling, het derde spoor op technologie en het laatste en vierde spoor op handhaving. De sporen zijn op te vatten als een cyclus die elkaar steeds logischerwijs opvolgen. Deze beleidscyclus sluit aan bij een belangrijk uitgangspunt van de WBP: namelijk zelfregulering. Het CBP heeft een adviserende en normerende taak bij de uitleg van wettelijke regels en voorschriften op een bepaalde verwerking. Deze adviserende taak wordt dringender naarmate

een verwerking meer complex, moeilijker inzichtelijk of een breed uitstralend effect heeft op het maatschappelijke veld. De (tijdige) onderkenning en analyse van technologische ontwikkelingen speelt dan ook een belangrijke rol bij de uitoefening van de wettelijke taken van het CBP. De uitkomsten van een dergelijke analyse bepalen in grote mate het beleid van het CBP, waaronder eventuele toepassing van de hem toekomende bestuursrechtelijke handhavende bevoegdheden.

Zoals gezegd is zelfregulering een belangrijk uitgangspunt van de WBP en daarmee ook binnen het beleid van het CBP. Als je de beschikbare middelen afzet tegen de scope van het toezicht van het CBP, dan valt direct op dat er sprake is van een onevenredige verhouding. Zo is het CBP de toezichthouder voor alle gegevensverwerkingen die bij en krachtens de wet plaatsvinden.¹¹ Bijna alle gegevensverwerkingen in bijna alle sectoren van onze samenleving vallen daarmee onder de toezichtstaak van het CBP.¹² Het is dan ook in het belang van het CBP zelf dat partijen die betrokken zijn bij de verwerking van persoonsgegevens, overgaan tot zelfregulering. Dit kan bijvoorbeeld door de ontwikkeling van branche- of sectorbrede gedragscodes die door het CBP van een goedkeurende verklaring kunnen worden voorzien. Daar waar sprake is van zelfregulering kan het CBP terugtreden als toezichthouder en zijn aandacht op andere aandachtsgebieden richten.

Eerder merkte ik al op dat voordat gedragsvoorschriften leiden tot normering in regelgeving van technologische ontwikkelingen, deze voldoende uitgekristalliseerd moeten zijn en niet langer onderhevig moeten zijn aan snelle veranderingen. Voordat er sprake kan zijn van normering door regelgeving, zal er, wettechnisch bezien rechtsonzekerheid bestaan, omdat noodgedwongen moet worden teruggevalen op algemene rechtsbeginselen. Om de rechtszekerheid te vergroten zouden technologische ontwikkelingen bij uitstek het terrein kunnen vormen van zelfregulering. Steun voor deze opvatting kan worden gevonden in de gedachte dat de ontwikkelaars van een technologie eveneens een goed inzicht hebben in de kansen, maar ook bedreigingen voor de bescherming van persoonsgegevens. Voor deze verantwoordelijken is zelfregulering verder van belang, omdat de WBP niet altijd eenvoudig, duidelijk en toegankelijk is. Eenvoud, duidelijkheid en toegankelijkheid zouden wel gewenst zijn, maar zijn vermoedelijk niet mogelijk, gezien de veelvormige en snel complexer wordende praktijk van gegevensverwerkingen en de veelheid van sectoren. De oplossing ligt dan in vormen van zelfregulering die recht doen aan de maatschappelijke variëteit.

Organisaties hoort men natuurlijk direct roepen dat zelfregulering kosten met zich meebrengt, terwijl tegelijkertijd het risico op 'ontdekking van de overtreding' klein is. Het zijn daarmee nalevingkosten die ongewenst zijn vanuit

8 J.E.J. Prins, 'Acht gesprekken over privacy en aanpalende belangen', in: *Zeven essays over informatietechnologie en recht*, ITeR reeks nr. 63, Den Haag: Sdu Uitgevers 2003, p. 53-105.

9 A. Roßnagel & J. Müller, 'Ubiquitous Computing – neue Herausforderungen für den Datenschutz. Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze', *Computer und Recht* 2004/8, p. 625-632.

10 Dit sluit aan bij wat het CBP 'privacy by design' heeft genoemd.

11 Art. 51 lid 1 WBP.

12 De kerstkaart die het CBP in 2005 rondstuurde gaf hier ook op ludieke wijze blijk van. De kaart rondstuurde uit een afbeelding van een eenzaam schip dat door een woelige zee vaart waarbij als tekst was toegevoegd dat het de 'kleinste toezichthouder met de breedste scope' was.

concurrentieoverwegingen (de rest doet het niet, dus waarom ik wel).

Er is veel op een dergelijk standpunt af te dingen.

Toegegeven, onder omstandigheden kan zeker op korte termijn een concreet kostenvoordeel te behalen zijn. Men bespaart immers een implementatie van regelgeving in de organisatie. Maar, voor een winstgedreven onderneming is het vertrouwen van de klant in de onderneming als voorwaarde voor winst minstens zo belangrijk. Recent onderzoek onder burgers toont bijvoorbeeld aan dat zelfs na de aanslagen van 11 september 2001 en daaropvolgend, burgers een groot belang hechten aan de bescherming van hun persoonsgegevens.¹³ Staatsveiligheid is een *big issue*, maar veiligheid heeft ook alles te maken met vertrouwen in een juiste omgang. Met het vertrouwen in een zorgvuldige behandeling zonder machtsongelijkheid. Veiligheid heeft ook te maken met het vertrouwen dat men niet benadeeld wordt doordat iemand over bepaalde (gevoelige) gegevens beschikt. Wat bijvoorbeeld als u een promotie op uw werk misloopt omdat uw 'concurrent' en collega beschikt over uw medisch dossier, met de inhoud waarvan hij u chanteert? Of wat als de pincode van uw bankpas in verkeerde handen komt? Denk aan de recente grootschalige veiligheidsincidenten bij Amerikaanse creditcardbedrijven, bij handelsinformatiebureaus of de herhaalde pogingen tot *phishing* via de website van een Nederlandse bank.

Veiligheid en vertrouwen oftewel het *compliant* zijn van een onderneming, is soms zelfs van direct belang voor de continuïteit van de onderneming. Als een klant vertrouwen in een onderneming heeft, komt die klant terug. Zo simpel is dat. En het gros van de ondernemingen ziet een klant graag nog een keer terugkomen. Het dunkt me dat de indirecte kosten die hierdoor bespaard blijven, een factor x groter kunnen zijn dan een concreet kostenvoordeel op de korte risicovolle termijn. Daarnaast vermindert zelfregulering ook de administratieve lasten hetgeen niet onbelangrijk is.¹⁴

3.2 *Funcitiescheiding en onafhankelijkheid*

Als het CBP op organisatieniveau wordt gezien, valt op dat een machtscheiding binnen zijn takenpakket op het eerste gezicht niet aanwezig is. Het CBP voert toezicht op regelgeving uit, voorts adviseert het over nieuwe regelgeving en tot slot kan het CBP uitspraak doen in bemiddelingen, klachten en ambtshalve onderzoeken. Het laat zich raden dat een nalevings- en handhavingstrategie zich niet goed verdraagt met een adviserende rol. Dit wreekt zich meer naarmate er sprake is van nieuwe technologische ontwikkelingen waarvoor het CBP conform zijn viersporenbeleid, eerst een analyse uitvoert en vervolgens normen zelfstandig formuleert en actief communiceert, voordat het tot handha-

ving kan overgaan. Mede om deze samenloop te ondervangen, heeft het CBP in april 2006 mandaatregelingen gepubliceerd¹⁵ die alsnog de vereiste interne scheidingen aanbrengen. Zonder deze mandaatregelingen zou de onafhankelijkheid van het CBP in het gedrang kunnen komen als het dubbelrollen blijft vervullen.

4 De drie machten

4.1 *Wetgeving*

Zoals in par. 2 al is behandeld maakt art. 80 WBP duidelijk dat de komende wetsevaluatie in het teken staat van technologische ontwikkelingen. Het is echter onduidelijk waar de wetsevaluatie toe gaat leiden. De WBP is in een digitale en sterk geautomatiseerde omgeving op zijn minst complicerend, ten minste dat is een veelgehoorde boodschap van betrokkenen én verantwoordelijken. Om het verouderde controledenken van de WBP te veranderen, zijn er af en toe klanken te horen waarin valt te beluisteren dat een zogenaamd 'Zweeds model' de toekomst zou hebben. Zeker in het licht van de dynamische omgeving waarin wij nu met zijn allen verkeren. Het 'Zweedse model' betekent niet meer of minder dan dat een ruime interpretatie wordt gemaakt van de uitzonderingen die de Richtlijn nr. 95/46/EG biedt waardoor vanuit het perspectief van de overheid, effectievere en efficiëntere bijdragen kunnen worden geleverd aan de bescherming van persoonsgegevens. Hierbij stapt men over naar een 'misbruikstelsel' waarbij alledaagse verwerkingen niet meer onder de regels voor gegevensbescherming vallen. Men kan dan slechts naar de rechter stappen indien men vindt dat er sprake is van 'improper intrusion of privacy'. Alleen die verwerkingen van persoonsgegevens die worden opgenomen in een database vallen dan nog onder de wet. De nadruk komt dan meer te liggen op de afweersfunctie van de wetgeving dan op de zorgvuldigheidsnormen van de wet. Vermeldingen van personen in tekstbestanden, het gebruik van digitale beeld- en geluidsopnamen of e-mailcorrespondentie zouden dan niet langer meer onder het bereik van de wet vallen. Het spreekt voor zich dat als er in Nederland wordt overgegaan tot het aanbrengen van veranderingen in het model van de WBP, dit voor rekening komt van de wetgever en dat het CBP daar geen invloed op zal hebben.

Mocht de wetsevaluatie leiden tot voorstellen tot aanpassing van de WBP, dan zal technologie niet als enige een rol spelen, dan wel zal technologie moeten worden gezien tegen de achtergrond van waarden waarvan wordt aangenomen dat deze een rol spelen binnen de WBP. Als waarden achter de WBP kunnen onder meer worden beschouwd de bescherming van de persoonlijke levenssfeer, gelijke behan-

¹³ Zie onder meer het rapport 'Burgers en hun privacy' van TNS NIPO Consult, februari 2005. Dit rapport is te downloaden van de website van het CBP <www.cbweb.nl>.

¹⁴ Administratieve lasten voor het bedrijfsleven zijn de kosten voor het bedrijfsleven om te voldoen aan informatieverplichtingen voortvloeiend uit wet- en regelgeving van de overheid. Het gaat om het verzamelen, bewerken, registreren, bewaren en ter beschikking stellen van informatie (zie ook <www.actal.nl>). Door middel van zelfregulering kunnen de lasten van informatiever-

plichtingen verminderen door standaardisatie en normalisatie via bijvoorbeeld gedragscodes.

¹⁵ Het betreft de besluiten 'Besluit mandaat en machtiging secretariaat Cbp' en 'Besluit mandaat en machtiging voorzitter en andere leden Cbp', *Stcrt.* 28 april 2006, 83. Verder betreft het de regelingen 'Regeling taakverdeling en onderlinge vervanging Cbp', *Stcrt.* 28 april 2006, 83; 'Regeling volmacht en machtiging beheer afdelingshoofden, coördinatoren en controller Cbp' en 'Regeling mandaat beheer directeur Cbp', *Stcrt.* 11 april 2006, 72.

deling, individuele autonomie binnen bepaalde grenzen, informationele gelijkheid en het voorkomen van onrechtvaardigheid en schade. Ieder van deze aspecten kan een zelfstandige rol spelen bij het beoordelen van technologieën op hun merites.

4.2 Rechtspraak

De bijzondere rechtsgang naar de civiele rechter waarvoor de WBP een regeling geeft, is bepaald niet laagdrempelig. Zo zijn er al veel procedures gevoerd over het recht op inzage bij Dexia Bank N.V. waarbij de verschillende gerechten weinig uniformiteit lieten zien in de procesformaliteiten en de Raad voor de Rechtspraak noodgedwongen instructies moest uitsenden. Ook zijn er problemen met de executie van uitspraken door betrokkenen, omdat hiervoor, in tegenstelling tot de hoofdzaak, wel juridische expertise en bijstand van specialisten vereist is. Verder is het griffierecht voor een civiele procedure op grond van de WBP op dit moment € 245. Tot slot loopt een betrokkene een procesrisico doordat het mogelijk is in de kosten van de procedure van de verantwoordelijke te worden veroordeeld (al gauw ongeveer € 900).

Behandeling van een geschil door het CBP is dan ook gemakkelijker en goedkoper. Zo kan een betrokkene ten aanzien van de steeds complexer wordende gegevensverwerkingen het naadje van de kous overlaten aan het CBP. Het CBP zal helemaal in de zaak duiken en deze uitpluizen om zich een beeld te vormen en een afgewogen oordeel uit te spreken. Een uitspraak van het CBP heeft echter geen rechtens afdwingbare gevolgen. Voorts is een gevaar van geschillenbeslechting door het CBP dat de (klassieke) uitvoerende macht die door de tenuitvoerlegging van de WBP en het CBP wordt vertegenwoordigd, te veel 'op de stoel van de rechter' en dus van de rechtsprekende macht, gaat zitten.

In dat opzicht doet zich dan ook de vraag voor of het CBP niet de bevoegdheid moet krijgen tot het starten van procedures en het kunnen interveniëren bij de Europese rechter. Het CBP laat daarmee rechtspraak over aan de rechtsprekende macht en kan zich meer concentreren op zijn uitvoerende rol. Op dit moment is de situatie aldus dat het CBP niet zelfstandig een procedure kan starten als het constateert dat dit wel wenselijk zou kunnen zijn in het belang van de rechtsontwikkeling. Ook kan het wenselijk zijn dat het CBP zelfstandig een procedure start om op te komen voor de belangen van een collectief van betrokkenen als die dreigen te worden benadeeld door onrechtmatig handelen van een specifieke verantwoordelijke.

4.3 Beleid

Het CBP hanteert graag zijn beleid om vast te houden aan een tweedelijnspositie. Daarmee creëert het evenwel tegelijkertijd een spanning ten aanzien van het streven naar rechtszekerheid bij de toepassing van nieuwe technologieën. Moet het CBP zich nu concentreren op grote(re) maatschappelijke ontwikkelingen (burgerservicenummer, Diagnose Behandel Combinaties, ov-chipcard) en de rest zo veel mogelijk buiten de deur houden? Of komt het op voor iedere burger van wie de gegevens eens een keer onrechtmatig zijn verwerkt? In dat licht kan worden opgemerkt dat

de overheid onder het mom van gemak (proactieve dienstverlening) gaat beschikken over een veelheid van elektronische identiteiten van burgers. Deze dienstverlening leidt, onder het samenstel van maatregelen, tot een identificatie- en authenticatie-infrastructuur en tot stroomlijning van gegevensbestanden: DigiD, elektronische identiteitskaart, biometrisch paspoort en authentieke registraties. Het CBP zal zich voor dit dilemma geplaatst zien en een keuze moeten maken. Is het David of is het Calimero?

5 Afronding

ICT heeft zeker gevolgen en bepaalde invloeden op gegevensbescherming. Zo staat er in 2006 en in 2007 een heleboel te gebeuren ten aanzien van de WBP en daaraan gerelateerde regelgeving. De WBP dient namelijk geëvalueerd te worden in het licht van de technologische ontwikkelingen. Mogelijkerwijs heeft deze evaluatie ook nog gevolgen voor de positie van de toezichthouder, het CBP. Zo valt te verwachten dat na de evaluatie van de wet, een (zelf)evaluatie van de uitoefening van taken door het CBP zal plaatsvinden.

De wetgever heeft in het verleden geworsteld met de ontwikkelingen in de ICT en het ziet er naar uit dat het dat ook in het heden en in de nabije toekomst zal blijven doen. Ontwikkelingen vliegen ons om de oren en zijn, afhankelijk van de eigen gekozen vlieghoogte, nauwelijks fatsoenlijk bij te houden. Laat staan dat de wetgever klip en klare normen zal weten te formuleren ten aanzien van het gebruik ervan.

ICT en gegevensbescherming hebben ook gevolgen en invloed op de scheiding der machten binnen de Nederlandse rechtsstaat. Ik ben hiertoe onder meer ingegaan op de mogelijkheid dat het achterblijven van een wetgever rechtsonzekerheid in de hand kan werken c.q. in stand kan houden. Wetgeving loopt immers per definitie achter de feiten aan. Feiten van vandaag zullen voor vele verantwoordelijken en betrokkenen dan ook niet kunnen wachten op die van morgen. De rechtszekerheid kan worden vergroot als organisaties niet wachten totdat normen juridisch uitgekristalliseerd zijn of als ze wachten op de wetgever. Organisaties moeten zelf actief zijn. Een vruchtbaar samengaan van ICT en gegevensbescherming kunnen organisaties heel goed zélf tot stand brengen. Bovendien passen naar mijn mening ICT en zelfregulering ook uitzonderlijk goed bij grondbeginselen van de WBP, zoals eigen verantwoordelijkheid, proportionaliteit en zorgvuldigheid.

Zelfregulering bij de toepassing van nieuwe technologische ontwikkelingen levert een positieve bijdrage aan de klassieke scheiding der machten. Het is de praktijk van vandaag dat wetten steeds minder gemaakt worden door het parlement, zoals het hoort, en steeds meer door de uitvoerende macht. De uitvoerende macht is nu eenmaal belast met het dagelijkse beleid en is veel meer in staat ontwikkelingen te doorgronden. De verschuiving van de wetgevende macht richting uitvoerende macht ligt nog meer op de loer wanneer er sprake is van nieuwe technologische ontwikkelingen. Hoeveel kamerleden zijn heden ten dage in staat technologische ontwikkelingen te doorgronden én te normeren? Zelfregulering waarborgt dat de uitvoerende macht van de overheid niet wetgevend tussenbeide hoeft te komen.