



Universiteit
Leiden

The Netherlands

Overheid en persoonsinformatie

Schmidt, A.H.J.

Citation

Schmidt, A. H. J. (1994). Overheid en persoonsinformatie. Retrieved from <https://hdl.handle.net/1887/3263>

Version: Not Applicable (or Unknown)

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/3263>

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

2. Overheid en Persoonsinformatie

A.H.J. Schmidt, H. Franken*

1. INLEIDING

De WPR is na een lange voorbereiding tot stand gekomen. Aan de basis stond algemene ongerustheid in de samenleving in verband met toegenomen automatisering van overheidsadministraties die leidde tot gevoelens 'van machteloosheid en van vrees aan een anonieme macht onderworpen te raken'.¹ Deze gevoelens uitte zich bij de algemene volkstelling van 1971 in verzet tegen de wettelijke verplichting inlichtingen te verstrekken. Na een periode van 18 jaar treedt de WPR in werking (1-7-1989). Intussen zijn genoemde machteloosheid en vrees ook gericht op privaatrechtelijke organisaties. In dit hoofdstuk beperken we ons tot persoonsinformatie bij organisaties met een publiekrechtelijke taak.

De bespreking van juridische kaders van overheidsinformatievoorziening leidt vrijwel steeds naar een hoog niveau van abstractie. Dorbeck-Jung gaat uit van de beginselen van de democratische rechtsstaat en de normerende-, instrumentele en waarborgfunctie van het bestuursrecht.² Franken introduceert beginselen van behoorlijk IT-gebruik³ en relateert die aan de algemene beginselen van behoorlijk bestuur. In dit hoofdstuk willen we uitgaan van een concrete vraagstelling en bezien welke juridische verplichtingen door de maatschappelijke ontwikkelingen met betrekking tot automatisering worden vereist. Dit betekent dat we zullen aangeven waarom een aantal juridische beginselen zo'n belangrijke rol speelt, terwijl we zullen besluiten met enkele suggesties voor de ontwikkeling van een meer praktisch gerichte benadering.

* Mr A H J Schmidt is universitair hoofddocent bij de afdeling Recht en Informatica van de Rechtenfaculteit Leiden en verbonden aan het onderzoeksinstituut Recht & Beleid van deze Faculteit

Prof mr H. Franken is hoogleraar in de Inleiding tot de rechtswetenschap en het Informaticarecht aan de Rijksuniversiteit Leiden en in de Juridische Informatica aan de Rijksuniversiteit Groningen

1 H H de Vries. 'De achtergronden van de Wet persoonsregistraties' in *Recht en Computer*, H Franken, H W K. Kaspersen en A H de Wild (eds), 1992, p 243

2 B R Dorbeck-Jung, Het juridische kader van de overheidsinformatievoorziening, in D Beekhuis en M J W. Beltman (red). *Informatievoorziening binnen de overheid*, UT, Enschede 1992, CBOO reeks, nr 79

3 H Franken, Overheid, informatietechnologie en recht - een gevarendriehoek? in. P H A Frissen, A W Koers en I Th M Snellen (red.) *Orwell of Athene? Democratie en informatiesamenleving*. Sdu, 's-Gravenhage 1992 H Franken, *Kanttekeningen bij het automatiseren van beschikkingen* Pre-advies voor de vereniging voor Administratief Recht (VAR), Alphen aan den Rijn 1993

Als concreet uitgangspunt nemen we een feitelijke situatie in gedachten. Het privacyvraagstuk is de laatste tijd vooral in beweging onder invloed van de maatschappelijke opvattingen over *toezicht* op de naleving van de eis tot bescherming van de persoonlijke levenssfeer. Daarbij geldt dat de overheid zelf evenzeer onderworpen dient te zijn aan toezicht op de naleving van deze eis als de individueel of collectief optredende burger.

Stel nu, dat de Minister van Binnenlandse Zaken behoefte heeft aan een indruk van de mate waarin door het politiepersoneel wordt 'bijgeklust'. Mag de minister van de fiscus een inkomensoverzicht vragen? En als de Minister van BiZa dit vraagt, mag de Minister van Financiën het overzicht dan ook geven? Als het overzicht vervolgens is verstrekt, mag de Minister de burgemeesters daarvan op de hoogte stellen? En als de burgemeesters op de hoogte zijn, hoe dienen zij met de informatie om te gaan? Wat moeten zij doen als een politie-ambtenaar inzage vraagt in deze over hem geregistreerde persoonsgegevens?

We stellen ons de volgende gang van zaken voor:

1. BiZa trekt een bestand met Sofi-nummers en NAW-gegevens uit zijn administratie en geeft dit aan Financiën met het verzoek om informatieverstrekking,
 2. Financiën verstrekt de gevraagde gegevens aan BiZa,
 3. BiZa verstrekt deze gegevens (voor zover relevant) aan de burgemeesters.
- Daarbij zullen we nagaan welke juridische belemmeringen deze gang van zaken kunnen beïnvloeden.

Het recht met betrekking tot informatievoorziening aan, binnen en door de overheid is onvoldoende uitgekristalliseerd om op de genoemde vragen onmiddellijk een stellig antwoord te kunnen geven. Privacy is een aspect dat bij deze informatievoorziening vaak een rol speelt, en de WPR en aanverwante wetten bieden daarbij een invalshoek. Het kan daarom verhelderend zijn om te bezien welke begrippen en regels uit de WPR 'oplichten' als mogelijk relevant voor het geven van antwoorden op de bovengenoemde vragen. Intussen zoeken we naar aanvullende regelingen waarin naar verwachting scherpere antwoorden kunnen worden gevonden.

2. TOEPASSELJKHEID VAN DE WPR

Mag de Minister van Binnenlandse Zaken aan de fiscus een inkomensoverzicht vragen?

Vragen staat vrij; de WPR laat zich hierover niet uit. Bij de eerste vraag vallen we onmiddellijk terug op beginselen: kan het informatieverzoek worden geconstrueerd als behorend tot de taak van de Minister van Binnenlandse Zaken? Via de ministeriële verantwoordelijkheid voor het politiebestel en via de verantwoordelijkheid van burgemeesters voor de door de politie te handhaven openbare orde kan de vraag worden gerekend als behorend tot de ministeriële taken. Daarbij geldt, dat de wijze waarop de minister zijn beheersverantwoordelijkheid uitoefent wordt bepaald door het politiek-maatschappelijke klimaat van het moment. Technische beperkingen bestaan niet meer. De mogelijkheid is daar. De

doelbinding van persoonsregistraties, één van de ankers van de WPR (artikelen 4, 6, 11 en 18), haakt zich in het drijfzand van de politieke agenda

We nemen aan dat de minister uit de personeelsadministratie van het departement een bestandje met naam-adres-woonplaats gegevens (of liever nog sofi-nummers⁴, die worden gehanteerd voor fiscaal inhoudingsplichtigen) trekt waarin de politie-ambtenaren zijn opgenomen. De Minister van BiZa mag dit bestandje aan de Minister van Financien verstrekken ingevolge artikel 14 WPR

Als de Minister van BiZa fiscale informatie vraagt, mag de Minister van Financien de betreffende gegevens dan verstrekken?

Het Sofi-NAW bestandje wordt door de Minister van BiZa aan de Minister van Financien aangeboden met het verzoek de inkomsten van deze personen te melden voorzover zij uitkomen boven de inkomsten waarvan de fiscus is ingelicht via de loonadministraties van de gemeenten. Mag de Minister van Financien dat overzicht aan zijn collega ter beschikking stellen?

Wanneer we naar de WPR kijken lijkt artikel 11 op het eerste gezicht een hindernis op te werpen gegevens aan een derde worden slechts verstrekt voor zover dat voortvloeit uit het doel van de registratie, wordt vereist volgens een wettelijk voorschrift of geschiedt met toestemming van de geregistreerde. Nu is het doel van de fiscale administratie niet het vaststellen van bijklussen door politiefunctionarissen, maar het aangeven hoeveel belasting ze (eventueel inclusief bijklussen) moeten betalen. De gevraagde informatieverstrekking wordt evenmin vereist ingevolge een wettelijk voorschrift en het vragen (en verkrijgen) van toestemming van de geregistreerden zou de hele onderneming van zijn zin beroven. Artikel 11 WPR werpt een hindernis op.

Artikel 18 lid 3 WPR is evenwel een tot de overheid gerichte speciale bepaling die aan artikel 11 derogeert uit registraties van *houders met een publiekrechtelijke taak* kunnen desgevraagd gegevens worden verstrekt aan *personen of instanties met een publiekrechtelijke taak*, voor zover zij die behoeven voor de uitoefening van hun taak en de persoonlijke levenssfeer daardoor niet onevenredig wordt geschaad. Deze constructie via de artikelen 11 en 18 lid 3 WPR hanteert de Minister van Justitie ten aanzien van de gegevensverstrekking van de fiscus aan de Informatiseringsbank⁵.

Wanneer we deze zienswijze overnemen dan heeft de Minister van Financien twee vragen te beantwoorden alvorens hij het verzoek kan honoreren. (1) is de informatie nodig voor de uitoefening van de taak van de Minister van Binnenlandse Zaken en (2) wordt de persoonlijke levenssfeer van de geregistreerden onevenredig geschaad door de eventuele informatieverstrekking?

De eerste vraag is niet alleen een staatsrechtelijke, maar vooral ook een politieke kwestie. De tweede vraag betreft een afweging die alleen gemaakt kan worden, wanneer bekend is wat de Minister van BiZa met de verstrekte informatie zal gaan doen. Wellicht is daarin voorzien in de aanvraag tot verstrekking, analoog aan de toelichting die artikel 6 van het besluit IVR⁶ vereist voor meer structurele vormen van informatieverstrekking. Maar zelfs dan, wanneer het

4 Zie voor een nadere behandeling van het Sofi-nummer in het kader van koppeling de bijdrage van Zwenne en Van Wezel in dit boek.

5 *Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies*, TK 1991-1992 nrs 145-146, p 14.

6 Besluit informatievoorziening in de rijksdienst 1990, *Stcrt* 20, 1991.

doel bekend is, vallen we voor de afweging zelf terug op algemene beginselen van behoorlijk bestuur

We achten het aannemelijk⁷ dat een zuiverder juridische constructie ten aanzien van derdenverstrekking door de fiscus wordt bereikt door artikel 67 AWR in de beschouwingen te betrekken. Berkvens betoogt elders in dit boek dat de ruimte die artikel 67 lid 2 AWR aan de Minister van Financien biedt om uitzonderingen te maken op de algemene geheimhoudingsplicht (ex artikel 67 lid 1 AWR) wordt beperkt door de afwegingen van artikelen 11 en 18 lid 3 WPR. Inhoudelijk leidt dit niet tot verschillen.

Juridisch technisch heeft dit nog heel wat voeten in de aarde. Artikel 67 lid 1 AWR verbiedt het verder bekend maken van informatie dan nodig is voor de heffing of de invordering van enige rijksbelasting. Lid 2 geeft de Minister van Financien de bevoegdheid hiervan ontheffing te verlenen. Deze ontheffing heeft een dubbele relatie met de bescherming van de persoonlijke levenssfeer: allereerst berust de algemene plicht tot geheimhouding van de fiscus op de overweging dat informatievergaring zou worden bemoeilijkt wanneer de informatie-verstrekking de burger niet op de afscherming van zijn persoonlijke gegevens zou kunnen rekenen, vervolgens spelen overwegingen van bescherming van de persoonlijke levenssfeer een rol bij de afweging die moet worden gemaakt wanneer ontheffing van de geheimhouding toch wordt verleend.⁸ Bij het verlenen van de ontheffing moeten vandaag de dag vanzelfsprekend eveneens de afwegingen van artikel 18 lid 3 WPR worden gemaakt.⁹

De conclusie is, dat we ook voor de beantwoording van de tweede vraag bij algemene beginselen belanden. Zowel het antwoord op de vraag of de Minister van BiZa de gegevens mag vragen, als het antwoord op de vraag of de Minister van Financien deze mag verstrekken komt te rusten op de algemene beginselen.

Als het overzicht is verstrekt, mag de minister de burgemeesters op de hoogte stellen?

Laten we aannemen dat de Minister van BiZa het overzicht van de fiscus heeft gekregen, nadat hij zijn redenen heeft uiteengezet. Het gaat om informatie die het uitvoeren van een interne bestuurszaak (toezicht) mogelijk maakt. De Minister van BiZa wil onderzoeken of, en zo ja, in welke mate er door politiefunctie-narissen wordt bijgeklust omdat hij van oordeel is dat aan die informatie een indicatie kan worden ontleend voor intern beleid. Hij heeft het *voornemen*

7 Evenzo J Berkvens AWR-WPR recombinant De privacyreglementen van de belasting dienst, *Computerrecht* 1991/3, pp 111-119

8 Het besluit Instructie informatieverstrekking (IIV) van 16-12-1982 gaf tot voor kort relevante richtlijnen. Dit besluit is inmiddels vervangen door het besluit Voorschrift informatie-verstrekking (VIV 1993). In onze casus gaat het om een politiek gevoelige zaak, zodat ingevolge art 2.1.2 VIV 1993 het verzoek om informatie wordt beoordeeld door de Minister van Financien (via de directie AFZ) en volgens de criteria van de art 3 lid 1^o 4 lid 4 VIV.

9 Dit dient overigens ook te gebeuren langs de weg van de geheimhouding. Volgens een uitspraak van de Afdeling Rechtspraak RvS van 26 juli 1984 (V-N 1985, p 184, punt 2) wordt art 67 AWR zodanig geïnterpreteerd dat de criteria van art 10 van de WOB van toepassing zijn. In lid 2, sub d en e worden als elementen voor de belangenafweging zowel het belang van inspectie, controle en toezicht als het belang van de eerbiediging van de persoonlijke levenssfeer als criteria voor afweging gegeven.

om burgemeesters van die gemeenten waar het bijklussen structurele vormen lijkt te hebben aangenomen die informatie te verschaffen opdat ze deze kunnen benutten om daarop maatregelen te baseren. Dit voornemen heeft hij evenwel niet in zijn verzoek aan de Minister van Financiën verwoord.

De Minister van Financiën heeft zijn informatie aan de Minister van BiZa via een netwerk ter beschikking gesteld in de vorm van een computerbestand. Ingevolge artikel 1 WPR gaat het om een *nieuwe* persoonsregistratie en is de Minister van BiZa de houder daarvan. Uit artikel 2 blijkt dat de WPR van toepassing is. De registratie is aangelegd in overeenstemming met de artikelen 4 en 6 (er is een bepaald doel, als neergelegd in de redenen van het verzoek aan de Minister van Financiën; dit doel is niet in strijd is met de openbare orde of de goede zeden; de gegevens worden voor dit doel gebruikt); de persoonsregistratie is er een van het Rijk (artikel 17 WPR), hij is *noodzakelijk* voor de goede uitvoering van toezichthoudende taak van de houder (artikel 18 lid 1 WPR) en er zijn niet meer gegevens in opgenomen dan nodig is voor die taak (artikel 18 lid 2 WPR). Kortom: vragen staat vrij maar verzamelen (in beginsel) niet. Het is evenwel opmerkelijk dat geen van de beperkingen uit de WPR nog een punt van discussie oplevert nadat de vraag van de Minister van BiZa door de Minister van Financiën bevestigend is beantwoord.

Het is nog wel nodig dat het doel in een reglement wordt omschreven en dat dit reglement wordt bekendgemaakt en ter inzage gelegd (artikelen 19 en 20 WPR). Het valt aan te nemen dat de kennisgeving van eerste opname en het inzage- en copierecht -en daarmee de toestemming van de geregistreerde- achterwege kunnen blijven omdat artikel 30 sub d (het belang van inspectie, controle en toezicht door of vanwege overheidsorganen) een afwijking van deze verplichtingen mogelijk maakt.

De Minister van BiZa is van oordeel dat ingevolge artikel 11 WPR uit deze persoonsregistratie nu informatie aan een burgemeester mag worden verstrekt omdat zulks voortvloeit uit het doel van de registratie. Toestemming van geregistreerden acht hij daarom onnodig. Het gaat nu echter weer om derdenverstrekking tussen instanties met een publieke taak en daarom werpt artikel 18 WPR een drempel op: de gegevens mogen alleen *desgevraagd* worden verstrekt. Om het doel van de registratie te realiseren zal de Minister van BiZa de burgemeesters moeten bewegen hem om de informatie te verzoeken.

Zodra die horde is genomen is *hij* (de Minister van BiZa) degene die volgens artikel 18 lid 3 WPR het doel van de gegevensverstrekking moet afwegen tegen de schade voor de persoonlijke levenssfeer van de geregistreerden. Dat is een duidelijke bestuurlijke afweging die met behulp van beginselen van behoorlijk bestuur moet worden gemaakt - deze afweging heeft *in feite* natuurlijk al aan het begin van de rit plaatsgevonden.

Als de burgemeesters op de hoogte zijn, moeten zij de informatie in een registratie opnemen of mag dat juist niet?

Zodra de burgemeester de beschikking heeft gekregen over het bestandje met fiscale gegevens over zijn politie-ambtenaren, begint alles opnieuw. De hele WPR lijkt opnieuw wakker te worden, hetgeen uiteindelijk leidt tot de burgemeester die als houder van een nieuwe persoonsregistratie een reglement moet opstellen en ter inzage leggen. De eerder gegeven overwegingen ten aanzien van doel en

noodzaak, alsmede die ten aanzien van de belangenafwegingen blijven van overeenkomstige toepassing. Daarvoor dienen alleen de algemene beginselen van behoorlijk bestuur tot richtsnoer.

Ten aanzien van het inlichten van de geregistreerden is een nieuwe situatie ontstaan: om maatregelen te kunnen nemen ten aanzien van onrechtmatig bijklussen zal de burgemeester de geregistreerden op de hoogte dienen te stellen. Ook deze informatieverplichting berust op algemene beginselen van behoorlijk bestuur.

3. DE WERKING VAN DE WPR VOOR PUBLIEKRECHTELIJKE PERSOONSREGISTRATIES NADER BESCHOUWD

(i) Het hiervoorgegeven gedachtenexperiment geeft de werking van de WPR in een scenario, waarin *ad hoc* wordt gekoppeld tussen persoonsregistraties van de overheid naar aanleiding van een politiek-maatschappelijke urgent geachte vraag. Welke vraag dit ook zal zijn, zij zal steeds worden gerekend tot de verantwoordelijkheid van één of meer ministers. Ondanks de centrale rol van de doelbinding in de WPR zal het in beginsel mogelijk zijn om publiekrechtelijke registratiehouders tot derdenverstrekking binnen de overheid te bewegen. Er wordt zo inderdaad *in feite* steeds een belangenafweging gemaakt. De belangenafweging tussen doel en schade aan de persoonlijke levenssfeer heeft immers al plaats gevonden doordat de vraag politiek gewicht heeft gekregen.

We concluderen daarmee dat de WPR weinig te bieden heeft voor de bescherming van de persoonlijke levenssfeer bij *ad hoc* koppeling van overheidsregistraties. Daartegenover staat dat de WPR, in die gevallen waarin de politieke kaarten nog niet zijn geschud, aan registratiehouders de plicht oplegt de afwegingen ter zake van doel van de registratie en de op te nemen gegevens enerzijds en privacybelangen anderzijds expliciet te maken, zodat deze eventueel aan het parlement kunnen worden voorgelegd. Bovendien zou hierover een advies van de Registratiekamer kunnen worden gevraagd.

(ii) Wanneer het doel van de registratie is goedgekeurd en de belangenafweging voor een derdenverstrekking is gehonoreerd, werpt de WPR geen inhoudelijke belemmeringen meer op voor de verdere verspreiding binnen de kring van overheidsorganisaties, zolang de verstrekking maar binnen het doel past en er geen specifieke wettelijke verboden werden geformuleerd. Heden ten dage kan die verspreiding efficiënt en in elektronische vorm worden verwezenlijkt.

De verplichting tot reglementering en bekendmaking volgens de artikelen 19 en 20 biedt de mogelijkheid van koppeling verantwoord af te leggen. We achten het echter niet uitgesloten dat de voordelen van de reglementsplicht van de artikelen 19 en 20 WPR ook hun keerzijde hebben. Door reglementering en bekendmaking worden *ad hoc* vragen in zekere zin geïnstitutionaliseerd. Daardoor kan de neiging bij houders ontstaan om *ad hoc* persoonsregistraties een meer permanente status te geven. Daarentegen kan het ook voorkomen, dat in de dagelijkse praktijk de resultaten van *ad hoc* koppeling van overheidsinformatie in het geheel niet worden gekwalificeerd als persoonsregistraties.

(iii) Gelet op, onder meer, het besluit IVR 1990 en het door het ministerie van Binnenlandse Zaken gepubliceerde *Handboek Normen voor de elektronische uitwisseling van persoonsgegevens* is niet de WPR een zorg die de koppelende overheid bezighoudt, maar gaat het om procedures die de kwaliteit van de geregistreerde gegevens bewaken en om standaards die de gegevensuitwisseling vergemakkelijken.¹⁰

(iv) Het onder (ii) en (iii) opgemerkte geldt evenzeer voor structurele gegevensuitwisseling tussen publiekrechtelijke persoonsregistraties. Doelbinding is daar meestal meer uitgekristalliseerd: de gegevensuitwisseling vindt plaats tussen geïnstitutionaliseerde diensten met een vastliggende taak of opdracht. Voor het oordeel van de informatieverstrekker of de vrager de informatie nodig heeft en of het doel opweegt tegen de schade aan de persoonlijke levenssfeer geeft het Besluit IVR 1990 een criterium. Artikel 3 lid 5 stelt dat 'het leggen van verbanden tussen informatie over individuele objecten in verschillende informatiesystemen' -de terminologie sluit niet direct aan op die van de WPR- plaats vindt voor het vervullen van specifieke, formeel toegewezen taken en op grond van duidelijke, schriftelijk vastgelegde regels. De vraag is natuurlijk of dit gebeurt en of en hoe daarop controle plaatsvindt.

(v) Doelbinding van de registratie vormt een waarborg en een gevaar voor de persoonlijke levenssfeer.¹¹ Uit het Besluit gevoelige gegevens blijkt, dat het noodzakelijkheids criterium wordt aangehouden voor het registreren van gegevens betreffende godsdienst of levensovertuiging, ras, politieke gezindheid, seksualiteit of intiem levensgedrag en persoonsgegevens van medische, psychologische, strafrechtelijke of tuchtrechtelijke aard. Dat noodzakelijkheids criterium wijst op een afweging van belangen.

(vi) De sanctiebepaling van de WPR verwijst voor registraties van publiekrechtelijke houders naar de reglementeringsplicht. Aan deze plicht kan, wanneer men van modelreglementen uitgaat, eenvoudig langs geautomatiseerde weg worden voldaan zelfs op het moment, dat een opsporing of vervolging reeds is aange-

10 Minister van Binnenlandse Zaken, (1991). *BIOS II, de computer gestuurd*, TK 1990-1991, 20 644, nr. 15. Minister van Binnenlandse Zaken (1991). Besluit informatievoorziening in de rijksdienst 1990 (IVR), *Stcrt* Nr. 20, dinsdag 29 januari 1991. Ministerie van Binnenlandse Zaken, (1991). *Handboek Normen voor de elektronische uitwisseling van persoonsgegevens*, ISBN 90-5414-004-6. Ministerie van Binnenlandse Zaken, (1992). *Sectorale verwijzindex persoonsinformatie*, ISBN 90-5414-01305. Ministerie van Binnenlandse Zaken, (1992). *Handboek Normen voor de elektronische uitwisseling van persoonsgegevens, Deel 2 implementatie aspecten*, ISBN 90-5414-007-0. Ministerie van Binnenlandse Zaken, (1993). *Handboek Normen voor de elektronische uitwisseling van persoonsgegevens, Deel 4 bouwstenen voor berichten*, ISBN 90-5414-017-8.

11 F. Kuutenbrouwer, *Wanneer computers koppelen*, Inaugurele rede, Deventer 1990. A.H.J. Schmidt, Staats- en administratiefrechtelijke implicaties van EDI, in: R.E. van Esch en C. Prins (red.), *Recht en EDI*, Serie Recht en Praktijk, nr. 68, Deventer 1992. Tjetske Gerbranda (red.), *Zelfidentificatie munderheden*, Working Paper Nr. 41, Leyden Institute for Law and Public Policy, 1993. J A G M. van Dijk, Privacynormen bij koppeling van computerbestanden, *Informatie en Informatiebeleid*, Vol. 11, 1993, nr. 1

vangen¹² Het is daarom niet ondenkbaar, dat de preventieve werking van de reglementsplicht voor overheidsorganisaties een illusie is

4 BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

De WPR is destijds op de politieke agenda geplaatst omdat maatschappelijke vrees bestond voor aantasting van de persoonlijke levenssfeer door de overheid. We verstaan hier onder de persoonlijke levenssfeer de ruimte voor burgers om zich vrij te bewegen en te ontwikkelen in het maatschappelijk verkeer (*informationele privacy*). Deze ruimte is groter naarmate het vertrouwen (tussen burgers onderling en tussen burger en overheid) groter is. Naarmate het vertrouwen afneemt, neemt de behoefte aan reglementering toe.

De werking van de WPR toont aan, dat reglementering lang niet altijd een oplossing biedt. Wanneer we onder ogen trachten te zien *wanneer* er sprake is van schending van de persoonlijke levenssfeer door de overheid, springen drie situaties in het oog.

(i) *Onrechtmatige afweging*

Doelbinding en het resultaat van de afweging als bedoeld in artikel 18 lid 3 kunnen in strijd zijn met algemene rechts- of bestuursbeginselen. Hier heeft de WPR weinig meer aan individuele burgers te bieden dan schadevergoeding achteraf. Op dit punt moet worden vertrouwd op de staatsrechtelijke mechanismen die de rechtsstaat overeind houden. Daarbij kan de Registratiekamer een bijdrage leveren door zich in de discussie te mengen.

(ii) *Onrechtmatig gebruik*

Doelbinding en afweging zijn behoorlijk geformuleerd en afgewikkeld, doch de registratie wordt in feite *voor een ander* doel gebruikt. Ook hier heeft de WPR weinig te bieden. Er zijn geen relevante sanctiebepalingen zolang aan de reglementsplicht is voldaan. De individuele burger moet zich wenden tot de rechter met een beroep op de algemene zorgvuldigheidseis die hem toch al ten dienste stond in zijn verhouding tot de overheid. Een praktisch probleem zal hier vrijwel steeds de bewijsvoering zijn. Het is niet altijd noodzakelijk en daarom weinig aannemelijk dat een beschikking zal worden gemotiveerd op een wijze waaruit kan worden afgeleid dat een persoonsregistratie wordt gebruikt voor een ander doel dan waarvoor zij is ingericht. De motivering hoeft het motief niet steeds te dekken.

(iii) *Onjuiste informatie*

Doelbinding en afweging zijn behoorlijk uitgewerkt en de registratie wordt overeenkomstig het doel gebruikt, maar de informatie in de registratie is niet in overeenstemming met de werkelijkheid. Hier biedt de WPR rechten tot kennisneming en verbetering. Daarvan zal evenwel op praktische gronden alleen in

12 Zie ook het sjabloon achtige model voor privacyreglementen binnen de overheid zoals beschreven in de bijdrage van Berkvens. Een dergelijke modelmatige aanpak vervult één van de voorwaarden voor efficiënte computerondersteuning bij het vervaardigen van individuele reglementen.

zeer ernstige gevallen gebruik worden gemaakt omdat er voor de burger veel tijd en inspanning mee gemoeid zijn.

Inmiddels is voldoende opgehelderd waarom in de discussies over persoonsregistratie door de overheid de beginselen van de democratische rechtsstaat en de algemene beginselen van behoorlijk bestuur een overwegende rol spelen. Voor de eerste twee van de drie genoemde probleemgebieden vormen zij de afsluiting. Voor het derde probleemgebied gelden de algemene beginselen van behoorlijk bestuur vooral als kader dat ertoe bijdraagt het aantal fouten te verminderen.

Het is daarom van groot belang dat de beginselen van behoorlijk bestuur ten aanzien van het opzetten en hanteren van persoonsregistraties worden uitgewerkt in beginselen van behoorlijk IT-gebruik.

5. BEGINSLEN VAN BEHOORLIJK GEBRUIK VAN INFORMATIETECHNOLOGIE (IT-GEBRUIK)

Dat onrechtmatige aanleg en onrechtmatig gebruik van persoonsregistraties in strijd zijn met algemene beginselen van behoorlijk bestuur spreekt vanzelf. Daarmee zijn we er evenwel nog niet: de vraag wat onder onrechtmatige aanleg en gebruik moet worden verstaan is niet eenduidig te beantwoorden. Voor het gedachtenexperiment hebben we een voorbeeld gekozen dat daarvan een illustratie biedt. In hoeverre gaat het de burgemeester aan dat ambtenaren van gemeentepolitie bijklussen? En verder, als het hem aangaat, hoe komt hij aan de relevante informatie en hoe gaat hij daarmee om? De moderne middelen van informatietechniek bieden mogelijkheden, die speciale eisen stellen aan het beschikbaar stellen en houden van informatie met waarborgen voor de controle van de produktie en het gebruik. We kunnen deze eisen in een aantal categorieën benoemen en daarmee specificaties aanduiden van algemene bestuursbeginselen, die bij het gebruik, de beschikking en de controle met betrekking tot informatie een rol spelen. We noemen deze normatieve criteria algemene beginselen van behoorlijk IT-gebruik.

In dit hoofdstuk zullen we deze beginselen toespitsen op het gebruik van persoonsinformatie door de overheid.

Beschikbaarheid

Bescherming van de persoonlijke levenssfeer vormt een inperking op de vrije toegankelijkheid van informatie en informatiesystemen. Zij kan echter in de huidige informatiemaatschappij alleen worden gegarandeerd als het gebruik van informatie controleerbaar is. Daarom geldt in een pluralistische samenleving, waar de vrije ontwikkeling van de persoon voorop staat, dat slechts de geïnformeerde burger een mondige burger kan zijn. Naast de grondwettelijk gewaarborgde vrijheid van meningsuiting is vrijheid van informatie een grondrecht, dat met zoveel woorden in artikel 10 EVRM is neergelegd. Daarom geldt: kennis moet vrij zijn, dat wil zeggen informatie moet beschikbaar, toegankelijk zijn. Dat wil natuurlijk niet zeggen, dat informatie steeds kosteloos ter beschikking moet worden gesteld. Het verwerven van kennis kost inspanning en daarmee heeft informatie een waarde in het economisch verkeer.

De wijze waarop informatie wordt overgedragen vormt vaak voorwerp van afspraken. De gegevensdrager is niet alleen meer papier, doch daartoe wordt tegenwoordig veel de telefoon, fax of electronic mail gebruikt. De afspraken over de methoden van verzending van berichten en de interpretatie daarvan leiden tot standaardisatie. Communicatie is pas efficiënt mogelijk als de diverse componenten van een informatiesysteem (apparatuur, software, verbindingsmiddelen) zijn gestandaardiseerd. Daartoe worden normen gedefinieerd met betrekking tot de functies van de systemen en de wijze van interactie met en tussen deze systemen. Deze normen gelden niet alleen de techniek. Ook voor de procedure en de inhoud van het berichtenverkeer moet eenduidigheid bestaan ten einde deze in beginsel voor de burger toegankelijk te doen zijn.

Allerlei vragen met betrekking tot toegankelijkheid van informatie, informatieplichten (vgl. artikel 4.2 lid 2 Awb) en onderzoeksplichten (vgl. afd. 4.1.2 Awb) zijn te kwalificeren met behulp van de gelijkheidseis en het formele zorgvuldigheidsbeginsel (artikel 3.2 Awb). Ook kan het in strijd zijn met het beginsel van fair play om informatie achter te houden of om relevante informatie terzijde te laten. In dit verband waarschuwen wij voor een mogelijk dictaat van de systeemtechnicus, die via de techniek enerzijds de informatieselectie beïnvloedt en anderzijds interpreterende regels kan implementeren.¹³ Door de noodzakelijke categorisering in informatiesystemen vallen bijzonderheden weg. Er vindt een vergroving plaats, die kan leiden tot een beperking van de belangenafweging (artikel 3.4 Awb).

Een waarschuwing geldt ook voor het vertrouwen, dat bij bestuursorganen zal bestaan ten aanzien van informatie die uit anderen hoofde reeds beschikbaar is. Het orgaan hoeft de burger daarover niet meer te horen, want het staat al in de computer. De technische verwerkings- en bewaarmogelijkheden geven een aureool van objectiviteit en onaantastbaarheid.

Vertrouwelijkheid

De eis tot exclusiviteit van informatie impliceert een zorgvuldig onderzoek en een redelijke en billijke belangenafweging. De grens met de beschikbaarheid van informatie moet nauwkeurig worden bepaald. Het spreekt haast vanzelf, dat aan de eis tot vertrouwelijkheid of exclusiviteit van informatie en informatiesystemen alleen kan worden voldaan als de houder van het informatiesysteem zorgdraagt voor de beveiliging daarvan. In recente wetgeving komt dit begrip twee keer naar voren. Artikelen 8 en 49 WPR stellen de eis van beveiliging van persoonsregistraties en in artikel 138a WvSr (computervrederebreuk) wordt het doorbreken van een beveiligingsmaatregel als voorwaarde voor strafbaarheid van de computerkraker aangemerkt.

Het is mogelijk de mate van beveiliging aan te geven op een schaal waarop de sterkte afneemt. Bovenaan staat dan de absolute beveiliging. Een situatie, waarop geen enkele inbreuk mogelijk is, behoort echter niet tot de realiteit. De volgende stap is een optimale beveiliging. Hierbij wordt gedacht aan de best denkbare situatie, die te realiseren is. De kosten van een dergelijk pakket maatregelen zullen prohibitief zijn. Men zal al gauw f 2,50 uitgeven om f 1,- te beveiligen. De eis van adequate beveiliging geeft aan, dat een afweging heeft plaatsgevonden tussen het te beveiligen belang en de genomen maatregelen. Artikel 8 WPR duidt

13 J.H. van Krefeld, *Computerbeschikkingen en rechtsstaatseisen*, in E.M.H. Hirsch Ballin en J.A. Kamphuis (red.) *Trias automatica*, Deventer 1985, p. 99.

op een dergelijke maat van beveiliging.¹⁴ In de Wet computercriminaliteit¹⁵ (vgl. artikel 138a WvSr) wordt verwezen naar een eis van minimale beveiliging: er moet sprake zijn van enige maatregel, die een drempel inhoudt tegen binnendringen. De eis is aldaar niet nader gespecificeerd dan dat voor het wederrechtelijk binnendringen een intellectuele inspanning is vereist. Tenslotte kennen we de symbolische beveiliging, bijvoorbeeld bestaande uit een bord met het opschrift 'verboden toegang'. Een zodanige vermelding op het computerscherm zal evenwel geen praktische betekenis hebben.

In dit kader is nog van belang, dat -bij amendement- in het Wetboek van Strafrecht een culpose variant is toegevoegd met betrekking tot het manipuleren (veranderen, wissen, onbruikbaar maken, toevoegen) van gegevens of het verspreiden van virussen (artikel 350b lid 1 respectievelijk lid 2 WvSr). Hiermee is een door de wetgever niet voorziene beveiligingsplicht geïntroduceerd, zowel voor de systeembeheerder, die onvoorzichtig is bij het voor gebruikers openstellen van zijn netwerk als voor die gebruikers zelf. Vooral bij koppeling van gegevens en systemen zal deze strafrechtelijke bepaling een rol kunnen spelen.

Artikel 2:5 Awb met een uitwerking in artikel 4:3 lid 1 geeft een nieuwe waarborg voor het vertrouwelijk omgaan met gegevens. Vooral bij de koppeling van systemen is het risico actueel, dat een beslisser buiten de betrokkene om gegevens ontleent aan een geautomatiseerd informatiesysteem en deze vervolgens zonder diens medeweten gebruikt bij het tot stand brengen van een beslissing. Een ander aspect is, dat de betrokkene zelf gegevens heeft aangeleverd, die niet worden gebruikt bij het nemen van het aangevraagde besluit, maar die 'achterblijven' in het systeem van het bestuursorgaan. Oude informatie kan men in een geautomatiseerd systeem gemakkelijk bewaren. De computer vergeet niet. Daarmee is een inbreuk mogelijk op de exclusiviteit, die de grens vormt voor de beschikbaarheid van informatie.

Integriteit

De informatie en de programma's waarin deze is verwerkt, moeten integer zijn. We geven hiermee een eis voor de inhoudelijke kwaliteit van een informatie(systeem) aan. Het systeem moet juist functioneren (doen wat het moet doen) en de gegevens en programma's moeten correct en volledig zijn. De informatie en programma's dienen in goede staat te zijn en overeen te stemmen met de opgestelde specificaties. De integriteit betekent ten aanzien van de output van een informatiesysteem, dat deze 'waar' is en dat men op de resultaten mag vertrouwen. Het gaat om de materiële waarheid van de output. Veel informatie wordt niet meer op documenten vastgelegd. Men moet er nu zeker van zijn, dat daardoor geen informatie ongemerkt verdwijnt of veranderd ter beschikking komt. Tevens moet de juistheid en volledigheid van de gegevens bij voortdurend worden gegarandeerd. Dit houdt een garantie in voor de actualiteit van de database. De integriteit van het informatiesysteem is te koppelen op de toepassing van het materiële zorgvuldigheidsbeginsel en het willekeurverbod (artikel 3:4 Awb).

Authenticiteit

De formele bewijskracht van computeroutput kunnen we aangeven met het begrip authenticiteit. Het gaat erom of verzonden berichten werkelijk van de af-

14 Zie MvA, p. 48.

15 Zie MvT bij w.o. 21551.

zender afkomstig zijn, of het juiste programma is geladen, of de inputgegevens door of namens de 'echte' aanvrager zijn verstrekt. De vraag naar de geldigheid is hier aan de orde. We zien hier een uitwerking van het formele zorgvuldigheidsbeginsel: zijn alle relevante factoren en omstandigheden in aanmerking genomen.

Flexibiliteit

Toepassingen van IT dienen flexibel te zijn, dat wil zeggen zij moeten gemakkelijk kunnen worden aangepast aan nieuwe gebruikseisen. Nieuwe regelingen en nieuwe feiten moeten gemakkelijk kunnen worden ingevoerd. Naast de actualisering van het te verwerken (input)materiaal moet ook een aanpassing van de programma's mogelijk zijn. Het gebruik van gegevens met behulp van nieuwe hardware, op een andere lokatie of in korter tijdsbestek mag geen verschillende output te zien geven. Tevens moeten informatiesystemen een zekere mogelijkheid bieden tot individualisering van toepassingen. Het kunnen rekening houden met of gebruik maken van individuele omstandigheden maakt immers vergelijking van gevallen mogelijk, een eis die voor besluitvorming met betrekking tot persoonsinformatie essentieel is. Hiermee blijkt flexibiliteit een uitwerking van het gelijkheidsbeginsel te zijn en verder te reiken dan de noodzaak om efficiënt met het systeem te kunnen werken.

Transparantie

De gebruikers van geautomatiseerde persoonsregistraties moeten aan de geregistreerden kunnen aangeven hoe en waarom ze tot een bepaalde output zijn gekomen. Er moet zichtbaar zijn, dat de technische maatregelen leiden tot de gestelde systeemdoelen. Het technische verwerkingsproces moge een black box zijn, de systeemdoelen moeten in ieder geval duidelijk kenbaar en begrijpelijk worden gepresenteerd. Ook de wijze waarop de door betrokkenen aangeleverde gegevens worden bewerkt valt onder een verantwoordingsplicht (artikelen 28 en volgende WPR).

Hier geldt, dat de eis van een kenbare en draagkrachtige motivering zowel slaat op de verantwoording van de systeemingénieur als op de controle van de uitvoerende ambtenaar. De eerstgenoemde wordt door het bestuursorgaan gedekt, dat ervan mag uitgaan dat de technici prestaties leveren op professioneel niveau. Voor de uitvoerende ambtenaar geldt, dat hij een hulpmiddel hanteert, waarvoor hij de toestemming of een opdracht heeft gekregen van de wettelijk bevoegde functionarissen. Uit het reglement moet blijken wie de bevoegde gebruiker of bewerker van het systeem is.

We moeten ons er wel van bewust zijn, dat bij de sterk toenemende complexiteit van informatiesystemen transparantie niet meer volledig kan zijn. Er mag dan mee worden volstaan dat de technische oplossingen de gestelde systeemdoelen realiseren, zoals de automobilist ervan mag uitgaan, dat bij indrukken van het gaspedaal de motor harder gaat lopen en de snelheid toeneemt.

Evenals voor de toepassing van de algemene beginselen van behoorlijk bestuur geldt zullen de hiergenoemde uitwerkingen voor situaties, waarin van middelen van moderne informatietechniek gebruik wordt gemaakt, niet steeds met elkaar sporen. De exclusiviteit van gegevens vormt een uitzondering op de eis van algemene beschikbaarheid van informatie en toegankelijkheid van informatie-

systemen. Individualisering leidt tot vergaande complexiteit van systemen, waarmee de transparantie wordt verminderd. Er zullen daarom afwegingen moeten plaatsvinden welk criterium in een individueel geval de voorkeur verdient. Deze afwegingen zijn gebruikelijk bij keuzen door functionarissen in een democratische en sociale rechtsstaat. De beginselen voor behoorlijk IT-gebruik zijn concretisering van waarden of rechtsbeginselen als informatievrijheid, vrijheid van meningsuiting, contractsvrijheid, openbaarheid van bestuur, bescherming van de persoonlijke levenssfeer of het verbod van discriminatie.

De overheid moet bij het gebruik van de toepassingen van IT op de naleving van deze beginselen kunnen worden aangesproken. Als de overheid met behulp van de produkten van IT haar voorwaardenscheppende en controlerende taak beter kan uitoefenen, dient zij evenzeer de checks en balances te scheppen, waarmee haar nieuw toegevoegde potenties onder controle worden gebracht. Wij vatten controle dan op in de continentale betekenis: contre-rôle of tegenkoppeling. De beginselen van behoorlijk IT-gebruik vormen de criteria voor deze controle.

6. PRINCIPES VAN DE DEMOCRATISCHE RECHTSSTAAT

De overheid is in haar uitvoerende taken voortdurend bezig met persoonsinformatie. De informatisering heeft de vraag naar regulering van het gebruik van persoonsinformatie door de overheid een nieuwe impuls gegeven. De wet geeft algemene (WPR) en soms meer specifieke richtlijnen (bijvoorbeeld de Wet politieregisters, de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag, de artikelen 47 en 67 AWR). Daartoe zijn eveneens bestuursbesluiten (bijvoorbeeld het besluit IVR 90) en in nota's neergelegde 'interne' gedragslijnen of instructies gegeven (vgl. BIOS-2 en VIV 1993). Deze regelingen laten onverlet, dat in het geval van concrete rechtsvragen een grote betekenis toevalt aan algemene rechtsbeginselen. Het betreft hier niet alleen algemene beginselen van behoorlijk bestuur (zoals voor de afweging van artikel 18 lid 3 WPR) en grondrechten (de spanning tussen klassieke en sociale grondrechten, bijvoorbeeld bij het minderhedenbeleid), maar ook de principes die het voortbestaan van de democratische rechtsstaat moeten garanderen. Deze principes zijn ten gevolge van de informatisering in toenemende mate in het geding. In een complexe samenleving zijn de overheidsinterventies gecompliceerd. De uitvoering en handhaving van een complex overheidsbeleid dwingt tot veel omvattende dataverzamelingen. De informatisering stelt de overheid in staat het beleid steeds verder te verfijnen en te differentiëren waarmee de noodzaak tot controle toeneemt. Een controle die met behulp van de moderne middelen van informatietechniek ook steeds beter mogelijk wordt. Dat betekent meer nadruk op de vraag naar de legitimiteit van het overheidsoptreden en de scheiding van machten als uitgangspunt voor een systeem van 'checks and balances'.

Het blijkt nu, dat de WPR aan de burger geen bijzondere bescherming tegen de overheid biedt. Enerzijds omdat de centrale beperkende rol die door middel van de doelbinding in de WPR moet worden bewerkstelligd, slechts wordt bepaald door de effectiviteit van het overheidsoptreden, terwijl anderzijds de in de WPR aan de geregistreerde toekomstige rechten worden beperkt door de afwegingsmogelijkheden van artikelen 11, 18 lid 3 en 30. Daarvoor zijn algemene beginse-

len van behoorlijk bestuur de normatieve criteria, die voor het terrein van de overheidsinformatisering nader worden ingevuld door de toepassing van algemene beginselen van behoorlijk IT-gebruik. Beginselen, die in privaatrechtelijke situaties de zorgvuldigheidseis nader zullen gaan omlijnen.

7. EEN MEER PRAKTISCHE BENADERING

We hebben kunnen zien hoe het vraagstuk van de bescherming van de persoonlijke levenssfeer van de burger in relatie tot het aanleggen en gebruiken van persoonsregistraties door de overheid voortdurend de weg effent naar abstracte rechtswetenschappelijke beschouwingen vanuit grondrechten en algemene beginselen. Jurisprudentie is nog steeds niet tot ontwikkeling kunnen komen¹⁶, zodat de overbrugging van beginselen naar concrete situaties vooralsnog een kwestie is van juridische dogmatiek.

Het is de bedoeling van de WPR geweest dat de rechtspositie van de burger ten aanzien van het registreren en gebruiken van persoonsinformatie zou verbeteren. Tot op heden is dat doel verwezenlijkt ten aanzien van inzage en verbetering van geregistreerde gegevens. Minder succesvol is de WPR waar het gaat om het ontwikkelen van rechtspositionele duidelijkheid in verband met *onzorgvuldig gebruik van gegevens*. Hier ligt nu een belangrijke taak voor de rechter en voor de Registratiekamer.

De burger kan zich tot de rechter wenden naar aanleiding van concrete bestuurs-handelingen. De rechter kan (eventueel via de Registratiekamer) aan de betreffende overheden opdragen te onthullen van welke persoonsinformatie gebruik is gemaakt en op welke wijze de betreffende gegevens beschikbaar zijn gekomen. Tenslotte kan de rechter in concrete uitspraken de betekenis van de beginselen van behoorlijk IT-gebruik als toetsingsmiddel vaststellen. Het wordt tijd dat de inspanningen die zijn geïnvesteerd in het optuigen van een juridisch kader rond de persoonlijke levenssfeer in de juridische praktijk worden gehonoreerd.

16 L.F.M. Verhey [*Horizontale werking van grondrechten, in het bijzonder van het recht op de Privacy*, Tjeenk Wilink, Zwolle 1992] geeft een overzicht van jurisprudentie die de belangenafwegingen voor civielrechtelijke verhoudingen enigszins ophelderen (Hoofdstuk 8) Deze jurisprudentie berust in belangrijke mate op de horizontale werking. Een interessante vraag is nu deze. is deze jurisprudentie óók van belang voor publiekrechtelijke verhoudingen? Of. is horizontale werking van grondrechten, om Bervens' terminologie te lenen, recombinant?