

Registratiekamer

Bij de opslag en het gebruik van persoonsgegevens moet de privacy van iedereen voldoende worden gewaarborgd. Tevens moeten de wetten die daartoe zijn vastgesteld, worden nageleefd. Om die twee doelstellingen te bereiken is in 1989 de Registratiekamer ingesteld. In de rol van onafhankelijk toezichthouder wil de Registratiekamer een betrouwbare en toegankelijke gids voor de samenleving zijn. Zij denkt niet alleen na over relevante normen voor de bescherming van persoonsgegevens, zij ontwikkelt ze ook daadwerkelijk en communiceert erover. Door ook de toepassing van deze normen te bewaken, bepaalt de Registratiekamer mede het humane gezicht van de informatiesamenleving nu en in de toekomst.

Om haar taak als toezichthouder effectief te vervullen, heeft de Registratiekamer ervoor gekozen de bescherming van persoonsgegevens langs vier sporen te bevorderen: bewustwording, normontwikkeling, technologie en handhaving. Door voorlichting en verschillende vormen van communicatie met uiteenlopende doelgroepen probeert de Registratiekamer het privacybewustzijn te versterken en de normen onder de aandacht te brengen. In studies, maar ook in de adviezen die de Registratiekamer uitbrengt, worden nieuwe normen voor gegevensbescherming ontwikkeld en de bestaande wettelijke normen verder geïnterpreteerd en uitgewerkt. In dit kader stimuleert zij ook zelfregulering door branches of sectoren. Door onderzoek te doen naar ontwikkelingen en toepassingen van informatie- en communicatietechnologie probeert de Registratiekamer de kritieke momenten in beeld te brengen en aan te geven hoe de normen van gegevensbescherming in de techniek een vertaling kunnen vinden. Het sluitstuk vormt de doorwerking van de privacybescherming in de praktijk. Door privacyaudits en andere vormen van handhaving wordt deze doorwerking bevorderd.

In haar rol als toezichthouder adviseert de Registratiekamer de regering over beleid en wetgeving waarin de privacy van de burger bij de verwerking van persoonsgegevens in het geding is. Omdat gedragscodes regels geven hoe in sectoren persoonsgegevens gebruikt worden, toetst zij deze gedragscodes. Verder onderzoekt de Registratiekamer de inrichting en het gebruik van persoonsregistraties. Zij behandelt klachten over het gebruik van persoonsgegevens en bemiddelt in geschillen tussen burgers en organisaties. Ten slotte vertegenwoordigt de Registratiekamer Nederland in internationale overleg- en controleorganen

Ten geleide

Privacy is net als de ozonlaag: onzichtbaar, maar onmisbaar. Tien jaar meet de Registratiekamer, als toezichthouder op de privacywetgeving in Nederland, de dikte van de privacy-ozonlaag. Dat jubileum werd feestelijk gevierd in oktober 1999 in het Mauritshuis. Het is daarom verleidelijk op het decennium als geheel terug te blikken. Dat is echter niet de bedoeling van het jaarverslag 1999. Deze terugblik dient beperkt te blijven tot de activiteiten en publicaties van de Registratiekamer in het meest recente jaar van haar bestaan.

Het jaarverslag van de Registratiekamer bestaat, net als vorig jaar, uit zes hoofdstukken en acht bijlagen. In hoofdstuk 1 wordt in vogelvlucht een impressie gegeven van de activiteiten van de Registratiekamer in 1999. In de hoofdstukken 2, 3 en 4 vindt u een bespreking van drie thema's die in 1999 centraal stonden en waarvan verwacht mag worden dat ze ook de komende jaren nog volop in de belangstelling zullen staan. De reguliere activiteiten van de Registratiekamer zijn op hoofdlijnen weergegeven in hoofdstuk 5, volgens een indeling die parallel loopt met het ontwikkelde 'viersporenbeleid'. Hoofdstuk 6 gaat in op de veranderingen die de organisatie in 1999 heeft doorgemaakt. Overzichten van aangemelde persoonsregistraties, uitgebrachte adviezen, onderzoeksrapporten en achtergrondstudies, gepubliceerde artikelen en overige gegevens, vindt u in de bijlagen.

Dankzij de inspanning van alle medewerkers van de Registratiekamer worden persoonsgegevens in Nederland zo goed mogelijk beschermd. De gehele Registratiekamer ziet uit naar het moment dat zij, onder de Wet Bescherming Persoonsgegevens, haar rol als toezichthouder nog beter kan uitvoeren.

Wilt u naar aanleiding van dit jaarverslag op de hoogte blijven van de voortgang van de nieuwe wet, de activiteiten of de publicaties van de Registratiekamer? Dan kunt u putten uit diverse andere bronnen met informatie: het katern 'Berichten van de Registratiekamer' in het tijdschrift *Privacy & Informatie*, de uitsprakenbundel *Persoonsgegevens beschermd* en de internetsite van de Registratiekamer: www.registratiekamer.nl.

mr. P.J. Hustinx (voorzitter)

drs. J.J. Borking (lid)

dr. U. van de Pol (lid)

Inhoud

1 1999 in vogelvlucht

Thema's

2 De digitale consument

3 Voorbereiding op de nieuwe privacywet

4 Integriteitbevordering

5 Activiteiten van de Registratiekamer

Communicatie

Ontwikkeling van normen

Technology assessment

Handhaving

6 Organisatie

Bijlagen

1 Aanmeldingen

2 Adviezen

3 Onderzoeksrapporten

4 Achtergrondstudies & Verkenningen

5 Brochures en Informatiebladen

6 Publicaties in vakbladen en tijdschriften

7 Gedragcodes

8 Modelreglementen vastgesteld voor politieregisters

9 Documenten van de Werkgroep inzake de bescherming van persoonsgegevens
(artikel 29 van Richtlijn 95/46/EG)

10 Formatie 1995-1999

11 Activiteiten 1995-1999 in cijfers

1999 in vogelvlucht

De gecombineerde doorbraak van internet en mobiele communicatie betekent veel nieuwe mogelijkheden voor consumenten. Zo'n nieuwe situatie is aanleiding voor de Registratiekamer om de nieuwe positie van de consument in kaart te brengen. Daarom heeft zij in 1999 veel aandacht gegeven aan de positie van de consument op de digitale snelweg (zie thema 1).

Verder stond 1999 in het teken van de invoering van de nieuwe Wet bescherming persoonsgegevens (WBP). Een stap voorwaarts is dat de Tweede Kamer de nieuwe privacywet in november met algemene stemmen heeft aanvaard. De discussie in de Tweede Kamer heeft natuurlijk de volle aandacht van de Registratiekamer gehad. De Registratiekamer heeft in het verslagjaar veel aandacht aan de consequenties van de invoering van de wet besteed en heeft de nodige voorbereidingen getroffen (zie thema 2).

Tussen politie/justitie en bedrijfsleven wordt informatie uitgewisseld om criminaliteit te bestrijden. Het screenen op betrouwbaarheid van (rechts)personen is een belangrijk aspect van de samenwerking tussen deze twee partijen. De uit te voeren integriteitsonderzoeken gaan voor betrokkenen echter gepaard met inbreuken op hun privacy. Teneinde een zo goed mogelijk beeld van de bestaande integriteitinstrumenten te krijgen heeft de Registratiekamer in 1999 een rondetafelconferentie over screening in Nederland georganiseerd (zie thema 3).

Belangrijkste publicaties

In 1999 heeft de Registratiekamer haar rapport *Informatieverstrekking door de fiscus - ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving* aan Staatssecretaris Vermeend van Financiën en de Tweede Kamer aangeboden. In deze publicatie wordt geconcludeerd dat de toepasselijke wettelijke regeling voor de verstrekking van persoonsgegevens door de fiscus - in het licht van privacywetgeving - niet meer up-to-date is. De Registratiekamer acht het gewenst dat daarin - in het verlengde van de herziening van het belastingrecht - wordt voorzien.

Publieke en private instellingen voor werk en inkomen werken steeds vaker samen. Uitvoeringsinstellingen, sociale diensten en arbeidsbureaus bieden onder het credo 'Samenwerking Werk en Inkomen' al gezamenlijk hun diensten aan in Centra voor Werk en Inkomen (CWI's). In de publicatie *Werken met gegevens* heeft de Registratiekamer de mogelijkheden en grenzen van deze samenwerking in CWI's geïnventariseerd en biedt zij enkele vuistregels voor de praktijk bij deze samenwerking.

Het gebruik van klantgegevens voor marketingdoeleinden was het onderwerp van een studie die in 1999 leidde tot de publicatie *Koning Klant*. In dit rapport geeft de Registratiekamer aan hoe de normen en regels van de Wet bescherming persoonsgegevens van toepassing zijn op de verwerking van consumentgegevens en hoe het economisch belang van organisaties bij het verwerken van die gegevens moet worden afgewogen tegen het privacybelang van de klanten.

De resultaten van een onderzoek van de Registratiekamer naar de inrichting en gebruik van het bevolkingsregister (GBA) in drie gemeenten zijn in 1999 bekendgemaakt. Uit het onderzoek bleek dat de gegevens van de burgers opgeslagen in de GBA onvoldoende beschermd zijn. De Registratiekamer gaat er van uit dat de situatie in die gemeenten een indicatie is voor de situatie in andere gemeenten in Nederland.

Ook nieuwe technologische ontwikkelingen die consequenties kunnen hebben voor de privacy van de burgers, hebben in 1999 de aandacht van de Registratiekamer gehad. Twee onderzoeksrapporten zijn op dit gebied gepubliceerd: *Intelligent Software Agents and Privacy*, opgesteld in samenwerking met de Canadese privacy toezichhoudende autoriteit voor Ontario, en *At face value: on biometrical identification and privacy*.

Actief op internationaal gebied

In de Werkgroep 'artikel 29' van de Europese privacyrichtlijn hebben alle Europese autoriteiten die op de privacy toezicht houden, zitting. De voorzitter van de Registratiekamer was de afgelopen vier jaar voorzitter van deze werkgroep. De problematiek van het gegevensverkeer met landen buiten de Europese Unie heeft in 1999 prominent op de agenda van de werkgroep gestaan. De richtlijn stelt hoge eisen aan de doorgifte van persoonsgegevens naar landen buiten de Europese Unie. In dit kader heeft de werkgroep meermalen advies uitgebracht over de dialoog van de Europese Commissie met de Verenigde Staten over de 'safe harbour' principes. Daarnaast heeft de werkgroep twee positieve adviezen uitgebracht over het beschermingsniveau van Zwitserland en Hongarije.

De Registratiekamer heeft een belangrijke bijdrage geleverd aan de activiteiten van twee subgroepen van deze werkgroep. De eerste was de Internet Task Force die vijf opinies heeft opgesteld over privacy op het Internet. De tweede was een subgroep die zich bezig hield met de beoordeling van communautaire gedragscodes. Naar verwachting zullen één of meerdere Europese gedragscodes in 2000 goedgekeurd worden.

De Registratiekamer vertegenwoordigt Nederland bij de adviescommissie bedoeld in artikel 18 van het dataprotectieverdrag van de Raad van Europa. De activiteiten van deze commissie waren in 1999 gericht op het opstellen van een protocol voor het verdrag waar twee onderwerpen aan bod komen: de derde landen problematiek en de rol van toezichhoudende autoriteiten. Deze twee onderwerpen waren niet (of niet voldoende) behandeld in de oorspronkelijke tekst van het verdrag uit 1981. Dit protocol moet gezien worden in het kader van de modernisering van het verdrag.

Sinds de invoering van de Schengen Uitvoeringsovereenkomst en de Europol Conventie neemt de Registratiekamer deel aan twee unieke vormen van internationaal toezicht. Beide verdragen kennen de instelling van een internationale onafhankelijke toezichthouder: voor het in Straatsburg gevestigde Schengen Informatie Systeem en voor de politieke systemen van Europol. Beide toezichthouders brengen een eigen jaarverslag uit.

Samenwerking met andere toezichhoudende autoriteiten wordt steeds belangrijker. Tijdens de lenteconferentie van Europese toezichhoudende autoriteiten in Helsinki heeft de Registratiekamer een rapport over audittechnieken gepresenteerd aan de Europese zusterinstellingen. Dit rapport werd opgesteld in nauwe samenwerking met de Spaanse *Agencia de Protección de Datos* en verder uitgewerkt tijdens een internationale workshop georganiseerd door de Registratiekamer. Zes landen en de Europese Commissie namen deel aan deze workshop, die in Den Haag gehouden werd.

De Registratiekamer heeft op verzoek van de Raad van Europa deelgenomen aan een officiële missie van de Verenigde Naties naar Kosovo. Tijdens de oorlog zijn de meeste bevolkingsregisters vernietigd; alle bewoners zullen daardoor opnieuw geregistreerd moeten worden en er zullen nieuwe identiteitsdocumenten uitgegeven moeten worden. De

Registratiekamer heeft bijgedragen aan het opstellen van nieuwe (privacyconforme) normen voor de bevolkingsregisters in Kosovo.

Ook landen buiten de Europese Unie tonen grote belangstelling voor de Europese privacywetgeving. Op uitnodiging heeft de Registratiekamer hierover voorlichting gegeven in de Verenigde Staten en heeft ze informatiesessies georganiseerd voor gasten uit onder meer Japan, China, Rusland, Kroatië en Slovenië.

De digitale consument

Veilig wonen, voldoende voedsel of kleding en betaalbare gezondheidszorg: zonder een goede organisatie en planning is het moderne leven ondenkbaar. Niet iedereen legt echter onmiddellijk een verband met de informatie die daarvoor nodig is. Voorstellingen van de informatiemaatschappij als een virtuele wereld vinden veel meer weerklank. Natuurlijk, door internet ontstaan nieuwe 'virtuele' activiteiten. De cyberspace-metafoor maskeert echter het zicht op de geleidelijke ontwikkeling naar een maatschappij die steeds meer afstemming van activiteiten, organisatie en planning veronderstelt.

Achter een verlanglijstje met parfum uit Frankrijk, sportschoenen uit Pakistan en videobanden uit de VS gaan wereldwijde organisatieketens schuil, die niet zouden kunnen functioneren zonder geavanceerde informatie- en communicatietechnologie (ICT). Digitale snelwegen zijn onmisbaar voor de coördinatie van alle activiteiten die voor een hedendaagse levensstijl benodigd zijn. Deze ontwikkeling is nog meer in een stroomversnelling geraakt met de gecombineerde doorbraak van internet en mobiele telecommunicatie. Via internet kunnen steeds meer aanbieders uit de hele wereld lokale markten bereiken. Omgekeerd krijgen consumenten toegang tot voorheen onbekende aanbiedingen. Mobiele telecommunicatie maakt alles nog bereikbaarder, ongeacht waar men zich bevindt. De hedendaagse technologie biedt ongekeerde mogelijkheden.

De enorme hoeveelheden informatie die nodig zijn voor de organisatie van een moderne samenleving hoeven niet noodzakelijk tot Orwelliaanse scenario's te leiden. Het doordringen van ICT in vrijwel alle aspecten van het dagelijks leven kan zowel meer zeggenschap en keuzevrijheid van de consument met zich meebrengen als inbreuken op diens privacy. Veelgehoord is de verwachting dat de consument bereid is zijn privacy op te geven in ruil voor de mogelijkheden van de nieuwe technologie. Toch blijft er gerede twijfel of vraag en aanbod naar privacy al hun evenwichtspunt hebben gevonden. Naar de overtuiging van de Registratiekamer ligt dat punt niet bij nul. We staan niet aan het einde van privacy, maar aan het begin.

Marktwerking en keuzevrijheid

Het kijken en kopen vindt steeds meer plaats in complexe, technologische omgevingen waarvan de werking voor de meeste consumenten niet bekend is. De mogelijke risico's nopen velen tot voorzichtigheid. Is een elektronische winkel wel betrouwbaar, kan ik er ruilen, zit er garantie op, komt mijn geld wel op de goede plaats? Op dergelijke vragen kunnen nog geen eenduidige antwoorden worden gegeven. In een dergelijke omgeving vertrouwen opbouwen valt niet mee.

Een complicerende factor is bovendien dat voor de commerciële transacties algemene communicatiesystemen worden gebruikt, waaraan tevens eisen dienen te worden gesteld uit oogpunt van betrouwbaarheid en integriteit. Een infrastructuur die ook van belang is voor het functioneren van de overheid, het onderwijs, de gezondheidszorg of van burgers onderling, kan derhalve niet geheel op de leest van het bedrijfsleven worden geschoeid.

De 'cybernaut' waant zich onzichtbaar achter zijn beeldscherm, dat hem vanaf welke plaats dan ook toegang biedt tot producten en diensten uit de hele wereld. Tegelijkertijd stelt hij zich in toenemende mate bloot aan observaties door zijn digitale omgeving. Het is bij dit alles dan ook van groot belang dat hij zicht houdt op wat er met kennis over zijn gedrag en voorkeuren gebeurt en dat hij ook in staat wordt gesteld daarop invloed uit te oefenen. Het gaat erom

voldoende evenwicht te behouden, zodat de voordelen niet overschaduwde raken door ongewenste ontwikkelingen.

Hoe meer bekend is van de behoeften en voornemens van de klant hoe beter daarop kan worden geanticipeerd, van het ontwikkelen van nieuwe producten tot het op maat aanbieden daarvan. Wie zittend op een terrasje een aanbieding voor goedkope filmkaartjes op het schermje van zijn mobiele telefoon krijgt, kan zich verheugen over de vergroting van zijn keuzemogelijkheden. De groei van het informatieaanbod leidt echter niet per definitie tot een verrijking van het leven; de enorme hoeveelheid informatie die dagelijks over de consument wordt uitgestort, wordt immers steeds triviale van inhoud. Op alle mogelijke manieren wordt getracht goederen en diensten onder de aandacht te brengen van personen die zich verder terugtrekken in hun persoonlijke leven. Televisieprogramma's die geen publiek trekken voor commercials raken in de verdrukking. Internet wordt gratis. Wie bereid is zijn beeldscherm aan te zetten om kennis te nemen van reeksen reclameboodschappen, kan daarmee zelfs geld verdienen. Maar niet iedereen staat altijd en overal open voor commerciële suggesties.

Monitoring van consumentengedrag kan weliswaar leiden tot meer keuzevrijheid voor de consument, maar kan ook van invloed zijn op de bestaande machtsverhoudingen. De huidige fusiegolf maakt de steeds nauwere verwevenheid tussen informatie- en telecommunicatie-/internetconcerns zichtbaar. De mogelijkheden van dergelijke conglomeraten om consumentengedrag te beïnvloeden moeten niet worden onderschat. De consument dient zich wel te kunnen beschermen tegen vormen van manipulatie en dwang.

Sinds de jaren tachtig plegen activiteiten van vrijwel iedere persoon routinematig te worden vastgelegd: bij het oppakken of aanzetten van de telefoon, het doen van boodschappen of het verrichten van betalingen. De digitale snelweg ondersteunt daarbij steeds meer activiteiten, van het doen van belastingaangifte tot het uitwisselen van foto's met familieleden overzee. 'Get wired' luidde de oproep van de internetgemeenschap aan buitenstaanders. Met de komst van mobiele internettoestellen zal dat veranderen in 'stay connected'. Hoever zijn we nog verwijderd van de consument die permanent met het net in verbinding staat, met zijn televisie, zijn koelkast, zijn creditcard en zijn digitale boodschappenlijstjes? Met biometrische identificatiemethodes zoals stem-, gezichts- of toetsaanslagherkenning kan men bij welke activiteit dan ook worden geïdentificeerd en gevolgd. Deze ontwikkeling roept de vraag op of er straks überhaupt nog menselijke activiteiten zijn die niet stelselmatig worden vastgelegd.

Het inspelen op individuele behoeften kent overigens ook nadelen. Wie zijn aanbiedingen te veel toesnijdt op elke individuele consument moet trachten de schijn van willekeur te vermijden. Klanten zullen ontevreden zijn als anderen om ondoorzichtige redenen voordeel krijgen en zij niet. Derhalve dringt zich steeds meer de vraag op of de huidige mate van detailkennis over individuele gedragingen wel onmisbaar is voor het dagelijkse management van bedrijven en instellingen. In de meeste gevallen houdt de differentiatie in het aanbod ook geen gelijke tred met de enorme hoeveelheden gegevens die met dat oogmerk worden bewaard. Het is bijvoorbeeld heel goed denkbaar iemand te adviseren over de beste van vijf mogelijke vakantiebestemmingen, zonder te beschikken over een compleet beeld van al zijn reizen in het afgelopen jaar. Dat noopt tot grotere selectiviteit bij het verzamelen van data.

Uit oogpunt van consumentenbescherming is markttransparantie een centrale voorwaarde. De consument zal niet alleen behoefte hebben aan prijs- en productvergelijkingen, maar zal zich in toenemende mate ook een indruk willen vormen van de privacyvriendelijkheid van de bedrijven die naar zijn gunsten dingen. Desgewenst kan hij dan zichzelf beschermen door zijn

gedrag daarop af te stemmen. Of de informatiemaatschappij zich in die richting zal ontwikkelen, is maar helemaal de vraag. Hier doet zich de eenzijdigheid in de ontwikkeling van de technologie voelen, gericht op het veelal onmerkbaar verkrijgen van inzicht in individueel consumentengedrag. Technieken waarmee de consument zijn privacy kan beschermen blijven daarbij ver achter. Daarbij moet niet alleen gedacht worden aan mogelijkheden om anoniem te kunnen rondkijken, maar ook aan mogelijkheden om meerdere pseudo-identiteiten aan te nemen zodat informatie uit verschillende 'levenssferen' niet zonder meer aan elkaar geknoopt kan worden. De voorlichting aan consumenten over deze aspecten is bepaald onvoldoende te noemen.

Het bedrijfsleven zweert bij 'Customer Relation Management', het verbeteren en uitbouwen van bestaande relaties met de klant. Eén-op-één marketing, het zoveel mogelijk toesnijden van aanbiedingen op individuele behoeften, maakt de aanbodzijde van de markt niet doorzichtiger. Dit in tegenstelling tot het individuele consumentengedrag. Marketing krijgt steeds meer trekken van een 'biechtstoelprocedure', waarbij alleen de marketeer zicht houdt op individuele reacties van consumenten, terwijl het niet meevalt individuele aanbiedingen met elkaar te vergelijken. Initiatieven die het aanbod meer transparant maken, zoals standaardisatie van websites of vergelijkende 'infomediaries' zouden deze ontwikkeling een andere richting kunnen geven.

Grondrechten in het digitale tijdperk

De regering besloot te bezien of de bestaande grondrechten moeten worden aangepast of uitgebreid gelet op de ontwikkelingen op het terrein van de informatietechnologie. Daartoe stelde zij de Commissie 'Grondrechten in het digitale tijdperk' in, onder voorzitterschap van prof. mr. H. Franken. De Commissie-Franken vroeg ook het oordeel van de Registratiekamer. De Registratiekamer onderschrijft de noodzaak van een grondige analyse van de gevolgen van de ontwikkelen op het terrein van de ICT en de fundamentele rechten en vrijheden van burgers. In een gedigitaliseerde wereld ontstaan controlemogelijkheden die bestaande vrijheden zoals de bewegingsvrijheid, vrijheid van meningsuiting of vrijheid van inmenging in de persoonlijke levenssfeer niet langer vanzelfsprekend doen zijn. De overheid legt telefoonbedrijven de verplichting op bij te houden op welke plaatsen iedere mobiele telefoon heeft aangestaan in de laatste drie maanden. Wie zich dat realiseert, zal niet meer onbevangen mobiel bellen. En alleen al de omstandigheid dat internetproviders in technische zin de mogelijkheid hebben alle communicatieverkeer inhoudelijk te controleren roept de vraag op of zij onwelgevallige uitingen niet dienen te weren.

In de afgelopen jaren zijn op zo'n schaal nieuwe gegevensverwerkende technologieën in gebruik genomen, dat niet meer van een reële keuzemogelijkheid voor de burger kan worden gesproken. Wie kan zich nog onttrekken aan computers die al het gebruik loggen, aan verkeersgegevens bewarende telecommunicatie- en internetbedrijven, aan het stevast meezenden van nummers van zowel afzender als geadresseerde, aan het gebruik van chipcards of in de toekomst aan biometrische identificatieprocedures voor wat dan ook? De mogelijke gevolgen van deze ontwikkelingen zijn voor de meesten moeilijk in te schatten.

De 'Internet Task Force', een werkverband van toezichthouders – zoals de Registratiekamer – in EU-verband, bestudeert momenteel in hoeverre de bestaande EU-privacyrichtlijnen, aanpassing behoeven in verband met de ontwikkelingen rond internet. Eén van de eerste resultaten van de task force was een aanbeveling aan producenten van hard- en software om zodanige producten op de markt te brengen dat het gebruikers mogelijk wordt gemaakt te voldoen aan eisen van databescherming. Zichtbaar gevolg in dit verband was bijvoorbeeld de

omslag bij Intel, die de standaardinstellingen van de Pentium III-processor wijzigde, zodat die niet meer steevast en onmerkbaar een nummer zou meezenden dat de gebruiker identificeert.

Activiteiten van de Registratiekamer in 1999

De Registratiekamer vroeg ook de aandacht van de Commissie Franken voor de mogelijke effecten van profilering voor de handelingsvrijheid van het individu. In toenemende mate zal de burger zich behandeld of beoordeeld zien op basis van groepskenmerken. Is bepaalde informatie nog wel toegankelijk voor wie niet tot de doelgroep behoort of komt men nog in aanmerking voor een geldlening of een mobiele telefoon als de vastgestelde kredietwaardigheidscore niet wordt gehaald? Verzekerd moet zijn dat een individu op zijn eigen merites wordt beoordeeld. Tegen vormen van oneigenlijke uitsluiting moet men zich kunnen verweren. De Registratiekamer acht het noodzakelijk te bezien of de grondrechtencatalogus in dit opzicht aanvulling verdient en ook of in het bestuursrecht en het contractenrecht aanvullende voorzieningen moeten worden getroffen. Het verbod op het verbinden van rechtsgevolgen aan geautomatiseerde beslissingen, zoals vervat in artikel 42 Wet bescherming persoonsgegevens (WBP) moet in dat licht worden bezien.

In de studie *Gouden bergen van gegevens. Over datawarehousing, datamining en privacy* uit 1998 was de Registratiekamer al ingegaan op de technieken waarmee profielen van personen worden gemaakt en beslissingen over hen worden genomen. Bij het onderbrengen van reeds aanwezige gegevens in een 'datapakhuis' wordt meestal niet onderkend dat de privacywetgeving voorwaarden stelt aan een dergelijk hergebruik. Niet bij alle gegevensverzamelingen kan er zonder meer vanuit worden gegaan dat een gebruik voor marketingdoeleinden verenigbaar is met het doel waarvoor gegevens werden verzameld. Een zorgverzekeraar die zijn gegevens over verzekerden analyseerde om aan kandidaten een diabetespas aan te bieden, ging naar het oordeel van de Registratiekamer te ver. Door meer openheid te betrachten en de betrokkenen zeggenschap te geven over een dergelijk gebruik had dat voorkomen kunnen worden. Het is verstandig al bij de bouw van een gegevenspakhuis privacybevorderende technieken in te bouwen. Niet alleen uit oogpunt van privacy, maar van een goed informatiebeleid in het algemeen.

De analysemethodes die bekend zijn als 'datamining' zijn er op gericht onvermoede relaties en patronen te ontdekken in enorme hoeveelheden data. Hiermee kunnen bijvoorbeeld voorspellingen worden gedaan zoals: deze klant gaat volgende maand een auto kopen. Een onderzoek naar de toepassing van creditscoring, waarmee bepaald wordt of iemand in aanmerking komt voor een levensverzekering, hypotheek of mobiele telefoon is in 1999 gestart. De resultaten zijn in 2000 te verwachten. Het zal duidelijk zijn dat voldoende concurrentie ongewenste neveneffecten, zoals willekeurige uitsluiting, zal minimaliseren. De afgewezenen gaat gewoon naar de concurrent.

Bij gebruik van dataminingstechnieken door de overheid is met het oog op de rechtmatigheid grote terughoudendheid geboden. Veelal kan de logica die aan een resultaat ten grondslag ligt, niet meer worden achterhaald. Op die manier kan toch bezwaarlijk een vergunning worden afgegeven of een belastingaanslag worden opgelegd. Ook bij monopolieachtige of ondoorzichtige marktverhoudingen zijn ongewenste vormen van uitsluiting of het maken van ongerechtvaardigd onderscheid niet ondenkbaar. In dit verband verdient ook de aan populariteit winnende etnomarketing bijzondere aandacht. De Registratiekamer bestudeert in hoeverre het mogelijk is bepaalde diensten en producten gericht aan te bieden aan etnische groepen, terwijl gewaarborgd is dat de daarvoor benodigde gegevens niet op discriminerende wijze kunnen worden gebruikt.

Er zijn diverse manieren om gegevens over klanten te verzamelen: klantenkaarten, bestelformulieren, voordeelbonnen, spaaracties en prijsvragen. De nieuwe WBP stelt voorwaarden aan de verwerking van die gegevens. In de studie *Koning Klant, het gebruik van klantgegevens voor marketingdoeleinden* worden de grenzen verkend tussen het economisch belang van bedrijven en het privacybelang van hun klanten. De voorwaarden die de WBP stelt zijn daarin verhelderd voor consumentenverhoudingen.

De Registratiekamer vindt het belangrijk om al in een vroeg stadium mogelijke implicaties van wereldwijd toegepaste technologie te bestuderen en waar nodig oplossingen aan te reiken. Momenteel investeert de ICT-industrie veel in de ontwikkeling van software, die namens ons kan handelen: zogenoemde 'Intelligent Software Agents' (ISA's). Een ISA kan bijvoorbeeld opdracht krijgen het goedkoopste vliegticket naar New York te zoeken. De 'agent' gaat zelfstandig het web op, bezoekt websites, kijkt en vergelijkt en meldt zich terug bij zijn opdrachtgever met het gevonden antwoord. Naarmate een ISA zijn opdrachtgever beter begrijpt zal zijn assistentie waardevoller zijn. De ISA zal dit 'leren' door voortdurende bijstelling van het profiel van zijn opdrachtgever.

Naar verwachting zullen ISA's onmisbaar worden bij de organisatie van het dagelijks leven in een netwerkmaatschappij. Maar voordat we allerlei taken laten uitvoeren door een elektronische bediende zal duidelijk moeten zijn hoe betrouwbaar hij is. Zoals een butler niet uit de school behoort te klappen over zijn baas, zo zal een ISA niet iedereen inzage moeten verlenen in het profiel met de wensen van zijn opdrachtgever. Al bij de ontwikkeling van deze technologie dient met dergelijke aspecten rekening te worden gehouden. In een gezamenlijke studie van TNO-FEL, de Registratiekamer en de Information and Privacy Commissioner van Ontario (Canada) zijn wegen aangegeven om 'agents' juist op een privacybevorderende manier in te zetten. De titel van het rapport is *Intelligent software agents and privacy*. Het is nu aan de ICT-wereld om agenten te ontwikkelen die ook het belang van de consument dienen.

Consument op de digitale snelweg beschermd?

De positie van de consument op de digitale snelweg blijft vooralsnog de aandacht houden van de Registratiekamer. Onderzoeken naar de feitelijke verwerking van persoonsgegevens rond het gebruik van internet, de interpretatie van normen, het adviseren van alle betrokken partijen en het stimuleren en aandragen van technische oplossingen staan in de komende periode centraal. Er is sprake van een complex krachtenveld waarin marktwerking niet steeds voor voldoende evenwicht zorgt. De eenzijdige ontwikkeling van communicatiesystemen in de richting van controletechnologie om redenen van staatsveiligheid, criminaliteitsbeheersing, bedrijfsbeveiliging of marketing van diensten behoeft correctie. Gebruikmaking van de digitale snelweg(en) behoort niet te zijn gebonden aan algemene en permanente identificatie- en registratieverplichtingen. De Registratiekamer stelt zich op het standpunt dat de consument in elk geval moet weten welke gevolgen de vaak routinematige verzameling van gegevens mogelijk kan hebben. Waar mogelijk moeten reële alternatieven worden aangeboden, ook in technische zin.

Vorbereiding op nieuwe privacywet

In de loop van 1999 zijn belangrijke stappen gezet op de weg naar een vernieuwing van het wettelijke kader voor de bescherming van de persoonlijke levenssfeer. Op 23 november 1999 heeft de Tweede Kamer met algemene stemmen het voorstel van de Wet bescherming persoonsgegevens (WBP) aanvaard. Dit vormde de positieve afsluiting van een intensieve discussie binnen en buiten het parlement, waaraan allerlei maatschappelijke organisaties een bijdrage hebben geleverd. Wanneer dit jaarverslag verschijnt, verkeert de behandeling van het wetsvoorstel in de Eerste Kamer in de eindfase. De invoering van de nieuwe regeling komt daardoor steeds dichterbij. Een goed moment voor een terugblik op de gevoerde discussie, een voorlopige tussenbalans en een indruk van de wijze waarop de Registratiekamer zich op de invoering van de WBP voorbereidt.

Privacy in de informatiemaatschappij

De indiening van het wetsvoorstel-WBP bij de Tweede Kamer in februari 1998 heeft geleid tot een intensieve discussie. Deze discussie kan worden geplaatst in het bredere perspectief van de veranderingen die onze samenleving als gevolg van de toenemende doorwerking van informatietechnologie de laatste jaren heeft doorgemaakt. Steeds meer is sprake van een samenleving waarin 'het verwerken van informatie' voor overheid, economie of welzijn een dominante factor wordt, ook wel aangeduid als 'informatiesamenleving'. In Europees verband wordt die term mede gebruikt om aan te geven dat het behoort te gaan om 'heel de samenleving' en de waarden waarop deze is gebaseerd. Bij de laatste Europese top in Lissabon stond dit thema prominent in de aandacht. De nadruk lag daarbij op de kansen die de nieuwe economie schept, maar ook is gesproken over het belang van een toereikende infrastructuur, onderwijs en sociale cohesie. Het scheppen van waarborgen voor de rechten en vrijheden van de burger behoort tot dezelfde basisvoorwaarden voor een evenwichtige ontwikkeling. De slotverklaring van de top laat zich daarover in soortgelijke bewoordingen uit.

De vernieuwing van het wettelijke kader voor de bescherming van persoonsgegevens is een wezenlijk onderdeel van de institutionele vernieuwing die nodig is om ontsporingen in de informatiesamenleving te voorkomen en zo nodig te herstellen. Het recht op privacy is een grondrecht dat in internationale verdragen is vastgelegd. Internationale organisaties, zoals de Raad van Europa en de OESO, zijn voorgegaan bij het ontwikkelen van waarborgen voor de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. In de Europese Unie heeft dat geleid tot de richtlijn waarvan de WBP is afgeleid. De richtlijn had ten doel de wetgevingen van de lidstaten op dit gebied te harmoniseren en te voorzien in een 'level playing field' voor producten en diensten die samenhangen met de verwerking van persoonsgegevens. De richtlijn biedt dus een breed gedeeld kader voor de activiteiten van overheden en bedrijven, ook als het gaat om het realiseren van de vele mogelijkheden die de nieuwe economie schept.

Er is alle reden om aan te nemen dat deze waarborgen ook op prijs worden gesteld door de personen om wie het gaat: consumenten, werknemers, patiënten en anderen van wie de gegevens, met of zonder hun instemming of medeweten, voor steeds meer doeleinden worden verzameld, verwerkt en gebruikt. Dat betekent: over ieder van ons, in de vele verschillende rollen die wij dagelijks spelen, zowel op het werk als daarbuiten. Recent onderzoek, zowel in Europa als in de Verenigde Staten, laat zien dat mensen blijven hechten aan de bescherming van hun persoonlijke gegevens, ook als zij in concrete situaties soms anders handelen. Dat geldt in het bijzonder voor de ontwikkeling van 'electronic commerce' en het gebruik van

internet. De vraag hoe het ‘vertrouwen’ van consumenten te winnen en te behouden is, ook en vooral bij de omgang met persoonlijke gegevens, vormt één van de punten van aandacht. Dit geldt niet alleen voor privacytoezichthouders, maar ook voor bedrijven die zich toelagen op de elektronische handel. Het realiseren van de grootse verwachtingen die op de top in Lissabon en elders zijn geformuleerd, zowel in maatschappelijke als in economische zin, hangt dan ook mede af van de wijze waarop wordt omgegaan met de privacyproblemen die de nieuwe tijd aan de orde stelt.

Zoals op veel terreinen gaat ook hier de kost voor de baat uit. Wie de privacy van burgers of consumenten – als grondrecht of als voorwaarde voor economische ontwikkeling – op prijs stelt, zal daarin moeten investeren. Dat moet op alle niveaus gebeuren: niet alleen in het wettelijke kader en bij de uitvoering op branche- of sectorniveau, maar ook in organisaties en bedrijven die dicht bij de basis staan. Er is op dat punt in de praktijk ook al veel gaande. In de loop van 1999 is de Registratiekamer betrokken geweest bij diverse projecten die vooruitlopen op de inhoud van de nieuwe wetgeving. Dergelijke voorbeelden van ‘good practice in privacy governance’ heeft zij als toezichthouder waar mogelijk gesteund.

Juiste balans in nieuwe wet

De uitgangspunten voor de nieuwe wetgeving mogen dan wel een breed draagvlak hebben, tijdens het afgelopen jaar is opnieuw gebleken dat discussie mogelijk is over de maatvoering en bepaalde onderdelen van de voorgestelde wettelijke regeling. Deze discussie is dan ook intensief gevoerd. De Registratiekamer heeft zich daarbij steeds op het standpunt gesteld dat een goede balans nodig is tussen wetgeving en zelfregulering en tussen extern toezicht en andere vormen van kwaliteitsbewaking. De inhoud van de richtlijn was hierbij voor haar een beslissende maatstaf. Ook de Registratiekamer hecht eraan niet meer te regelen dan nodig is: zij zoekt actief naar partners, bevordert zelfregulering, ondersteunt privacycodes van organisaties en bevordert ook op alle mogelijke andere manieren dat privacy op de verschillende maatschappelijke terreinen de aandacht krijgt die hij verdient. Rechten en plichten en voldoende middelen om deze af te dwingen zijn in een rechtsstaat echter nodig om belangenconflicten op te lossen. De Registratiekamer is tevreden dat met de WBP nu de juiste balans is gevonden tussen conflicterende belangen.

In de Tweede Kamer hebben alle fracties nog eens kritische opmerkingen gemaakt over de complexiteit van het wetsvoorstel en in het bijzonder over de moeilijke toegankelijkheid van de toelichtende stukken. De minister van Justitie heeft in dat verband de toezegging gedaan dat hij met een heldere handleiding voor de WBP zal komen. De kritiek in de Tweede Kamer bleek uiteindelijk mild, afgezet tegen eerdere voorstellen van belangengroeperingen om het wetsvoorstel in te trekken en een geheel nieuw voorstel in te dienen. De behandeling verliep bovendien in goede harmonie. Op aandrang van de Tweede Kamer is de WBP in de laatste fase op een aantal punten aangescherpt. Zo zijn de criteria voor ‘verenigbaar gebruik’ in het wetsvoorstel teruggekeerd, is het gebruik van ‘Privacy Enhancing Technologies’ (PET) in het kader van de beveiliging verankerd en is de mogelijkheid tot het opleggen van bestuurlijke boeten in geval van niet-aanmelding veilig gesteld. Van groot belang was verder de met algemene stemmen aanvaarde motie waarin bij de regering werd aangedrongen op het zoveel mogelijk stimuleren van PET bij de overheid.

De behandeling van de WBP heeft met dat al helaas langer geduurd dan de Europese richtlijn toeliet. De termijn voor invoering verliep reeds op 24 oktober 1998. Inmiddels heeft de Europese Commissie aangekondigd dat zij het Hof van Justitie in Luxemburg een uitspraak

zal vragen over het uitblijven van de nieuwe privacywetgeving in Nederland. Het blijft dan ook van belang dat de WBP nu spoedig tot stand komt en zo snel mogelijk wordt ingevoerd.

Ondanks verschillen grote mate van continuïteit

In de Wet bescherming persoonsgegevens worden in vergelijking met de Wet persoonsregistraties (WPR) nieuwe begrippen geïntroduceerd, verandert het object van regelgeving en wordt een ander systeem van materiële normen en formele eisen ingevoerd. Zo zullen alle normen en eisen van toepassing zijn op de 'verwerking van persoonsgegevens' en niet op het voeren van een 'persoonsregistratie', een verschil dat direct samenhangt met de technologische ontwikkeling en grotere behoefte aan bescherming in uiteenlopende situaties. Wie eenmaal deze verschillen met de WPR doorziet, ontdekt echter dat er in de praktijk een grote mate van continuïteit bestaat. Beginselen van rechtmatigheid, transparantie, doelbinding, proportionaliteit (de beperking van het recht op privacy mag niet onevenredig zijn in verhouding tot het nageleefde doel) en subsidiariteit (het nageleefde doel mag niet op een minder ingrijpende manier worden bereikt) en het toekennen van rechten aan betrokkenen zijn algemene beginselen uit de WPR en vormen eveneens de basis voor de nieuwe wet. Dat is begrijpelijk als men bedenkt dat de WPR en de WBP via de Europese richtlijn terugrijpen op dezelfde internationale basisbeginselen, vastgelegd in het Verdrag inzake dataprotectie van de Raad van Europa. Instellingen en bedrijven die hun privacybeleid nu op orde hebben, zullen dus ook onder de nieuwe wetgeving een voorsprong hebben.

Wel liggen accenten op een aantal onderdelen anders. Zo zijn de wettelijke normen al van toepassing bij het 'verzamelen' van persoonsgegevens en worden in dat stadium ook hogere eisen gesteld aan de transparantie van de gegevensverwerking voor de betrokkene. Dit zal tot gevolg hebben dat de betrokkenen beter in staat zullen zijn voor hun belangen op te komen. Naast deze aanscherpingen zal er ook sprake zijn van vereenvoudiging. Zo zal de procedure voor het doen van meldingen worden vereenvoudigd en zullen meer vrijstellingen gelden van de meldingsplicht.

Onder het regime van de WPR is de handhaving van de gestelde regels, met uitzondering van die over melding, grotendeels in handen gelegd van de geregistreerde of van organisaties die in zijn belang optreden. In de WBP zullen ook handhavingsbevoegdheden zijn toegekend aan het College bescherming persoonsgegevens (CBP), de nieuwe benaming van de Registratiekamer. Het CBP zal een bestuurlijke boete kunnen opleggen bij het niet-nakomen van de verplichtingen tot melding. Voor bepaalde verwerkingen waar een groter risico bestaat van inbreuk op de persoonlijke levenssfeer wordt een voorafgaand onderzoek geïntroduceerd. Het CBP zal op basis van dit onderzoek moeten besluiten of al dan niet een verklaring van rechtmatigheid van de verwerking kan worden afgegeven. Het nakomen van wettelijke verplichtingen zal verder zo nodig door toepassing van bestuursdwang of door oplegging van een last onder dwangsom kunnen worden afgedwongen.

Bevoegdheden die worden toegekend, scheppen ook verplichtingen. De uitoefening van de aan het CBP toe te kennen bevoegdheden zal op een zorgvuldige wijze moeten plaatsvinden. Zorgvuldig enerzijds in de zin dat de inzet van bevoegdheden slechts plaatsvindt als daartoe voldoende aanleiding bestaat en na een gedegen voorbereiding. Zorgvuldig ook in die zin dat goed wordt afgewogen hoe de beschikbare capaciteit het meest efficiënt kan worden ingezet.

Viersporenbeleid

Persoonsgegevens spelen bij een veelheid van maatschappelijke activiteiten een cruciale rol. Het toezicht op de manier waarop met die gegevens wordt gewerkt, omvat dan ook een breed

en gevarieerd takenpakket. Een toezichthouder op dit gebied zal nooit effectief kunnen zijn, uitsluitend door op te treden tegen geconstateerde overtredingen. De door de Registratiekamer eerder gekozen strategie langs vier sporen – bewustwording, normontwikkeling, technologie en handhaving – zal ook in de toekomst perspectief bieden.

De Registratiekamer investeert in contacten met organisaties en instellingen die zich verantwoordelijk voelen en tonen voor de privacybescherming op hun terrein. Hierdoor zijn tot dusver kansen gecreëerd om een voorlichtende en adviserende rol te vervullen in de beginfase van ontwikkelingen en projecten. Die vroegtijdige betrokkenheid biedt mogelijkheden om bij de realisatie daarvan wegen en oplossingen aan te geven die in overeenstemming zijn met de privacyregelgeving, ook waar het gaat om technologie die daarbij kan worden gebruikt. De nieuwe bepaling over beveiliging, artikel 13 WBP, biedt mogelijkheden voor een betere verankering van privacynormen in systemen en procedures en voor een systematische controle op de werking daarvan.

Een actieve opstelling op het punt van voorlichting en advisering kan naleving van de nieuwe privacyregelgeving bevorderen, maar zal overtreding daarvan niet uitbannen. Ook dan zal de inzet van handhavingsbevoegdheden door het CBP niet altijd nodig zijn, en zeker niet als de eerste optie. Privacyproblemen zijn vaak sterk ingekleurd door de specifieke omstandigheden binnen een bepaalde sector of branche. Klachten- of geschillencommissies die binnen zo'n sector of branche zijn ingesteld, blijken in veel gevallen in staat om hierbij tot een voor klager en overtreder bevredigende oplossing te komen. De mogelijkheid van geschillenbeslechting op een dergelijke wijze, mits voldoende onafhankelijk, is voorzien in het onderdeel van de WBP dat gaat over gedragscodes. Goede voorlichting en ondersteuning bij het ontwikkelen van normen binnen een sector of branche, kunnen er toe bijdragen dat het CBP zich in zulke gevallen kan opstellen als een tweedelijnsorganisatie.

Desondanks zal inzet van handhavingsbevoegdheden in bepaalde situaties niet te voorkomen zijn. Inzet van die bevoegdheden moet dan gezien worden als een uiterste middel, dat in de gevallen waarom het gaat, ook gerechtvaardigd zal zijn. Dat de inzet van die middelen met voldoende waarborgen op het punt van zorgvuldige voorbereiding en mogelijkheid tot het aanwenden van rechtsmiddelen omgeven dient te zijn, is in de WBP op verschillende plaatsen verankerd.

In het verlengde hiervan en mede naar aanleiding van de discussie in de Tweede Kamer is in de Registratiekamer het afgelopen jaar intensief nagedacht over het eigen functioneren als toezichthouder en de ervaringen die daarbij zijn opgedaan. Dat heeft er niet alleen toe geleid dat de bovenbedoelde 'viersporenstrategie' is bevestigd, maar ook dat daarbinnen ruimte is gevonden voor aanpassingen. Zo zijn wijzigingen doorgevoerd in het communicatiebeleid. De nieuwe aanpak op dit gebied legt meer nadruk op grote ontwikkelingen en reageert minder op incidenten. Daarnaast krijgen kennis van de praktijk en oplossingsgericht denken in het beleid van de Registratiekamer thans een zwaarder accent dan tevoren. Meer in het algemeen heeft een nuchtere bezinning op bestaande taken geleid tot meer selectiviteit bij het aanpakken van onderwerpen en het voornemen de Registratiekamer waar mogelijk meer te profileren als een tweedelijnsorganisatie. In het jaarplan 2000 heeft een en ander nadere invulling gekregen.

Goede en gerichte voorlichting

Wil inderdaad sprake zijn van continuïteit bij de overgang van WPR naar WBP dan zullen zowel de betrokken partijen in de maatschappij als de toezichthouder zelf daarop voorbereid moeten zijn. Dit vergt goede en gerichte voorlichting aan de verschillende maatschappelijke

sectoren, maar ook een scholing en toerusting van de organisatie binnen de Registratiekamer. Een en ander dient op zo'n manier gerealiseerd te worden dat de lopende zaken normaal doorgang kunnen vinden.

Natuurlijk zijn veel partijen ook nu al geïnteresseerd in de gevolgen van de WBP voor hun organisatie. Veel van deze partijen maakten gebruik van het telefonische spreekuur waar zij terechtkonden met vragen over de belangrijkste verschillen tussen de oude en de nieuwe wet. Naast deze reguliere voorlichting is de Registratiekamer in samenwerking met de ministeries van Justitie en Binnenlandse Zaken en Koninkrijksrelaties begonnen met de voorbereiding van een breed opgezette campagne die de WBP moet gaan introduceren bij het publiek. Het ministerie van Justitie is verantwoordelijk voor de ontwikkeling van een heldere handleiding over de inhoud van de WBP voor de praktijk. De Registratiekamer richt zich vooral op het benaderen van verantwoordelijken in diverse sectoren via hun betrokken koepelorganisaties teneinde langs die weg zoveel mogelijk te komen tot een toespitsing van de voorlichting op sectorniveau. In dat verband staat een breed scala van mogelijkheden ter beschikking. Onder meer kan worden gezorgd voor toegespitste presentaties en artikelen in vakbladen. De wensen van de diverse sectoren worden momenteel geïnventariseerd.

Op het moment dat de WBP in werking treedt, moet het CBP als toezichthouder gereed zijn om de toegekende taken uit te voeren. Te verwachten is dat het accent daarbij wat de nieuwe wet betreft, zeker in de eerste periode, zal liggen op voorlichting en bewustwording. Naast de nieuwe wet zal op grond van de overgangsbepalingen ook de oude wet nog enige tijd van toepassing zijn. Om te kunnen voorzien in de behoefte aan gerichte voorlichting, moet snel en effectief op vragen vanuit de maatschappij gereageerd kunnen worden. Voorwaarde daarvoor is dat kennis van de wet en de toepassing daarvan breed verankerd zijn binnen de organisatie. De voorbereiding daarvoor krijgt gestalte door de ontwikkeling van een systeem dat de wet zelf en de parlementaire geschiedenis kan ontsluiten, en door gerichte scholing van de medewerkers aan de hand van uiteenlopende casuïstiek. Bij het analyseren viel opnieuw op dat er naast verschillen ook veel overeenkomsten bestaan tussen de oude en nieuwe wet. Veel uitspraken die de Registratiekamer in het verleden gedaan heeft op grond van de WPR zullen zodoende hun waarde behouden.

Voorlichting en advisering zijn belangrijke onderdelen van de toezichthoudende taak, maar de naleving van de nieuwe regels ter bescherming van de persoonlijke levenssfeer zal soms met krachtiger middelen moeten worden bevorderd. Het voorstel van de WBP kent het CBP op dit punt bevoegdheden toe waarover de Registratiekamer op grond van de WPR niet beschikt. De uitoefening van deze nieuwe bevoegdheden zal op zorgvuldige en transparante wijze moeten plaatsvinden. Voor de huidige werkprocessen is, naast standaardisering en stroomlijning, op onderdelen aanpassing nodig. De uitwerking van oude en nieuwe werkprocessen, alsmede de vereiste voorzieningen om een mogelijke vermenging van taken tegen te gaan, zullen worden verankerd in het bestuursreglement dat op grond van de WBP is voorgeschreven. De inhoud van alle werkprocessen zal worden vastgelegd in protocollen.

Aanmelden

Evenals de WPR kent de WBP een verplichting om gegevensverwerkingen bij de toezichthouder aan te melden. Door het creëren van een voor alle maatschappelijke sectoren in beginsel gelijke aanmeldingsverplichting, door vermindering van de gegevens die over een verwerking moeten worden aangemeld, en door een substantiële uitbreiding van het aantal vrijstellingen, is gestreefd naar flinke vereenvoudiging van de aanmeldplicht. Door gebruik te maken van de technische mogelijkheden is op het punt van de administratieve

lastenverlichting nog meer winst te behalen. De Registratiekamer heeft daarom met het oog op de uitvoering van de WBP een diskette voor het doen van aanmeldingen ontwikkeld. Een prototype van deze diskette is inmiddels gereed. Deze kan ook worden gebruikt om te bepalen of voor een verwerking van persoonsgegevens een aanmeldingsplicht geldt of dat sprake is van een vrijstelling. De eindversie van de diskette kan worden gereed gemaakt zodra een datum voor het in werking treden van de nieuwe wet bekend is en de definitieve tekst van het Vrijstellingenbesluit beschikbaar is. Het wordt ook mogelijk de inhoud van de diskette te downloaden van de website van het CBP (www.cbpweb.nl). De houders van persoonsregistraties die hun registratie thans bij de Registratiekamer hebben aangemeld, zullen zoveel mogelijk gerichte informatie ontvangen over wat hun onder de nieuwe wet te doen staat.

Integriteitsbevordering

Screening is als instrument voor het toetsen van de integriteit sterk in opkomst. Een degelijke screening gaat echter gepaard met een aanzienlijke inbreuk op de privacy van de betrokkenen. Om deze reden volgt de Registratiekamer de ontwikkelingen rond screening kritisch. Haar uitgangspunt is dat screening als inbreuk op de privacy gerechtvaardigd kan zijn. Voorwaarden zijn dat er een evenwicht moet zijn tussen het reële belang van degene die opdracht geeft tot de screening en de hiervoor noodzakelijk geachte inbreuken op de privacy van betrokkenen. Waar mogelijk zal met minder ingrijpende alternatieven volstaan moeten worden om de privacyinbreuk voor betrokkenen binnen de perken te houden. Essentieel is ook dat de screening plaatsvindt volgens heldere toetsingscriteria en op grond van rechtmatig verkregen informatie. Van even groot belang is dat de screeningsprocedure voor de betrokkene kenbaar is en wordt omgeven met passende rechtswaarborgen. Een wettelijke screening dient met het voorgaande in overeenstemming te zijn. Onder deze voorwaarden kan een screening op aanvaardbare wijze plaatsvinden.

Screening bij overheid en bedrijfsleven

Naar aanleiding van de bevindingen van de Commissie Van Traa heeft de regering in november 1999 het wetsontwerp Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur (BIBOB)

ingediend. Voorgesteld wordt om een centraal bureau BIBOB in het leven te roepen om (rechts)personen te screenen op integriteit. Kenmerkend voor deze wet is dat de screening op integriteit door een landelijk bureau plaatsvindt aan de hand van privacygevoelige gegevens die uit veelsoortige informatiebronnen afkomstig zijn.

Vooruitlopend op de wet BIBOB heeft de gemeente Amsterdam een screenings- en bewakingsaanpak ontwikkeld bij de aanbesteding van grote bouwwerken. Een lokaal bureau onderwerpt toekomstige contractpartners in de bouwsector aan een integriteitsonderzoek. Deze aanpak is vooralsnog beperkt gebleven tot een (proef)screening voor een brug naar IJburg. In de nabije toekomst zal er ook op grotere schaal worden gescreend bij omvangrijke aanbestedingsprojecten van de Noord-Zuidlijn. Ook in Rotterdam zijn screeningsinitiatieven ontwikkeld. Zo wordt onder meer geëxperimenteerd met het screenen van bedrijven, waarbij de Minister van Justitie op verzoek van een bedrijf een integriteitsverklaring kan afgeven. Met behulp van deze verklaring kan het bedrijf zijn betrouwbaarheid aantonen.

Naast de overheid heeft ook het bedrijfsleven behoefte aan integere zakenpartners. Het gaat hierbij om klassieke methoden als creditscoring van toekomstige cliënten. Ook de aanleg van zwarte lijsten als integriteitsmethode is een al langer bekend fenomeen. In opkomst is de 'criminal audit' als screeningsmethoden voor zakelijke partners. Het gaat dan om het inschatten van bedrijfsrisico's. Aan de hand van opgestelde betrouwbaarheidsprofielen worden risicoanalyses van de cliënt gemaakt. De uitkomsten daarvan zijn beslissend voor de vraag of een bedrijf al dan niet, dan wel onder bepaalde voorwaarden met een cliënt een zakelijke relatie aangaat.

In het kader van publiek-private samenwerking heeft de Stichting Nationaal Platform Criminaliteitsbeheersing (NPC) het project informatie-uitwisseling tussen politie/justitie en bedrijfsleven opgezet. Het bedrijfsleven stelt met enig recht de vraag waarom de overheid wettelijke screeningsinstrumenten voor zichzelf reserveert. Dit project wil voor de praktijk van de informatie-uitwisseling tot beter hanteerbare en juridisch houdbare regels en

procedures komen. Dit speelt met name op het gebied van het onderzoeken van integriteit van rechts- en natuurlijke personen. Om deze reden heeft het NPC het onderwerp screening boven aan de agenda gezet. Het gaat hierbij met name om een onderzoek van de mogelijkheden voor uitwisseling van persoonsgebonden informatie tussen overheid en private sector ter bestrijding van de criminaliteit en ter bevordering van de integere samenleving. De Registratiekamer neemt aan de werkzaamheden van het NPC deel.

In de financiële sector zijn integriteitseisen aangescherpt. In dit kader wordt de betrouwbaarheid van (potentiële) beleidsbepalende en medebeleidsbepalende personen van financiële instellingen op meer diepgaande wijze getoetst. Teneinde de toetsing op betrouwbaarheid meer op elkaar af te stemmen is besloten tot intensieve informatie-uitwisseling. Het onlangs opgerichte financieel expertisecentrum (FEC), een samenwerkingsverband van onder meer financiële toezichthouders, belastingdienst, politie en openbaar ministerie, heeft een centrale rol gekregen bij het bevorderen van integer handelen in de financiële sector.

Normatief kader

Bij screening komt de persoonlijke levenssfeer van degene die hieraan wordt onderworpen, in het geding. Dit brengt mee dat een dergelijk onderzoek door de overheid moet voldoen aan de normen van artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 10 van de Grondwet (GW). In deze artikelen is het recht op privacy vastgelegd. Voor de aan screening inherente inbreuk op de persoonlijke levenssfeer dient een voldoende maatschappelijke noodzaak te bestaan en de inbreuk dient te zijn gebaseerd op een van de gronden die artikel 8 lid 2 EVRM hiervoor biedt. Voor zover er sprake is van een structurele screeningsvorm, ligt het voor de hand dat er een specifieke wettelijke voorziening voor getroffen wordt conform het bepaalde in artikel 8 EVRM en artikel 10 van de GW. In andere gevallen kunnen bestaande wettelijke voorzieningen toereikend zijn. In elk geval dient het beoordelingscriterium zo gericht mogelijk te zijn en de aard en de omvang van het onderzoek moeten gerelateerd zijn aan de kwestie waarop de screening betrekking heeft. Met minder in de persoonlijke levenssfeer ingrijpende alternatieve methoden moet worden volstaan, indien deze voor het beoogde doel toereikend zijn. Ten slotte dient de screening met speciale procedurele waarborgen omgeven te zijn. Slechts onder bovengenoemde randvoorwaarden is een inbreuk op het recht op privacy gerechtvaardigd.

Voor zover een screeningsvorm door specifieke wettelijke voorschriften genormeerd is, dient uiteraard de screening conform deze voorschriften verricht te worden. De Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag (WJD) en de Wet veiligheidsonderzoeken zijn hiervan voorbeelden. Voorts dient voorzover de verwerking van persoonsgegevens aan de orde is, screening in overeenstemming te zijn met de wetgeving met betrekking tot de bescherming van persoonsgegevens: de Wet persoonsregistraties en straks de Wet bescherming persoonsgegevens.

Ook voor zover er geen specifieke wettelijke voorziening aanwezig is voor screening, zijn overheidsinstanties en private marktpartijen gehouden aan de normen van het EVRM en de daarbij behorende privacybeoordeling. Deze doorwerking geldt in sterke mate voor de overheid en in minder sterke mate voor het bedrijfsleven. De nadere juridische invulling vindt in dat geval mede plaats aan de hand van het bovengenoemde privacykader.

Bij het screenen op integriteit neemt de WJD een centrale plaats in. Op verzoek van de aanvrager stelt de burgemeester van zijn woonplaats een onderzoek naar zijn antecedenten in

met het oog op het verkrijgen van een bepaalde functie. De burgemeester moet een verklaring omtrent het gedrag (v.o.h.g.) afgeven als de betrokkene geen of een voor de functie niet relevant strafrechtelijk verleden heeft.

In de praktijk gaat het met name om werkgevers die sollicitanten verzoeken een dergelijke verklaring over te leggen. Voordeel van de v.o.h.g. boven andere screeningsinstrumenten is dat de privacy van de betrokkenen niet of nauwelijks in het geding is. De partij aan wie de verklaring wordt overgelegd draagt immers geen kennis van de aan de verklaring ten grondslag liggende feiten en omstandigheden. De v.o.h.g. heeft met name door een wisselend beoordelingsbeleid van burgemeesters en door een beperkte toegang tot informatie die was opgeslagen in politieregisters, aan waarde ingeboet.

In de praktijk zagen werkgevers de WJD niet meer als een betrouwbaar screeningsinstrument. De regering heeft daarom besloten deze wet ingrijpend aan te passen. Deze wetwijziging maakt het mogelijk dat met de afgifte van een verklaring omtrent het gedrag op centraal niveau via heldere toetsingscriteria een afgewogen oordeel wordt gegeven over de integriteit van de aanvrager. Ook voor rechtspersonen kan een dergelijke verklaring worden afgegeven. De afgifte van de v.o.h.g. is niet slechts bij het aangaan van arbeidsrelaties mogelijk. Ook bij bijvoorbeeld het verstrekken van leningen of het aangaan van een koopovereenkomst kan de v.o.h.g. in de toekomst worden afgegeven. Ook de mogelijkheid om uit politieregisters te putten voor wat betreft actuele informatie over de aanvrager wordt uitgebreid.

Voor zover het nodig is een diepgaand screeningsonderzoek naar het (privé)leven van betrokkene en zijn omgeving te verrichten, biedt de Wet veiligheidsonderzoeken daarvoor de juridische basis. Dit onderzoek is mogelijk bij specifieke daar aangewezen functies bij de overheid en het bedrijfsleven. Deze screening is vanuit privacyoogpunt gezien de meest vergaande vorm van integriteitsonderzoek. Dit onderzoek wordt uitgevoerd door de BVD of onder mandaat van de BVD.

Activiteiten Registratiekamer

Gelet op de aan screening inherente inbreuk op de persoonlijke levenssfeer is screening op integriteit voor de Registratiekamer het afgelopen jaar een belangrijk thema geweest. Ook voor 2000 blijft het onderwerp op haar agenda.

Op verzoek van het NPC heeft de Registratiekamer een rondetafelconferentie georganiseerd over de bestaande en toekomstige screeningsinstrumenten in Nederland. Deelnemers waren onder meer afkomstig uit het verzekerings- en bankwezen, de landelijke en lokale overheid en forensische consultants. Tijdens de conferentie viel de deelnemers op dat de bevoegdheden om te screenen verspreid zijn over diverse wettelijke regelingen. De deelnemers aan de conferentie onderschreven dat screening een ingrijpende inbreuk kan maken op het privéleven van de hierbij betrokken personen. De Registratiekamer heeft in de publicatie Tegen het licht gehouden verslag gedaan van deze screeningsbijeenkomst. De uitgave gaat vergezeld van een 'röntgenfoto' van screenend Nederland. Hierop zijn de bestaande en toekomstige integriteitsinstrumenten van de aan de conferentie deelnemende personen en instanties in kaart gebracht. Voor de verdere ontwikkeling van het screeningsinstrumentarium kan deze beschrijving van de stand van zaken als uitgangspunt dienen.

De Registratiekamer is verder betrokken geweest bij de Amsterdamse initiatieven op het gebied van screening. Van de evaluatie van de activiteiten van de Wallenmanager heeft zij met belangstelling kennis genomen. Over de verlenging van zijn machtiging van de minister

van BZK om van de gegevens uit politieregisters kennis te nemen zijn diverse gesprekken gevoerd. Belangrijk hierbij is dat voor uitbreiding van activiteiten zoals door de Wallenmanager zijn ontplooid voldoende noodzaak bestaat in de situatie waartegen het gemeentebestuur wenst op te treden. In een brief aan het gemeentebestuur van Amsterdam heeft de Registratiekamer op hoofdlijnen ingestemd met de Amsterdamse screening- en bewakingsaanpak. Voor twee knelpunten heeft de Registratiekamer echter in het bijzonder aandacht gevraagd bij het verder ontwikkelen van de screeningsprocedure. In de eerste plaats dient het gemeentebestuur alsnog een machtiging te verkrijgen om politieke en justitiële gegevens te raadplegen teneinde de door ondernemingen opgegeven antwoorden te kunnen verifiëren. In de tweede plaats dient voldaan te zijn aan de aanmeldings- en reglementsverplichting van de WPR teneinde de te volgen procedure voor de betrokkenen transparant te maken.

De Registratiekamer onderschrijft het belang van een adequate bewaking van de integriteit in het bedrijfsleven en van de in Boek 2 van het Burgerlijk Wetboek (BW) geregelde toetsing op vennootschappen. Dat neemt niet weg dat beide moeten voldoen aan de randvoorwaarden die daaraan zijn gesteld uit een oogpunt van de bescherming van de persoonlijke levenssfeer van de hierbij betrokken personen. Vanuit deze privacynormen heeft de Registratiekamer de regering over het ontwerpvoorstel van Wet documentatie vennootschappen geadviseerd. Dit ontwerp heeft primair betrekking op de verwerking van gegevens. Deze gegevens worden verwerkt in het registratiesysteem Vennoot '98 van het Ministerie van Justitie voor het preventief toezicht op vennootschappen. Voorgesteld is om deze gegevens ook te gebruiken voor andere doeleinden, waaronder het voorkomen en bestrijden van misbruik en criminaliteit. Uitgangspunt voor de Registratiekamer is echter dat het ontwerpvoorstel slechts volgend en ondersteunend kan zijn ten opzichte van de bestuurstaken waarvoor Vennoot '98 wordt aangelegd. Hierin past niet het uitbreiden van bevoegdheden van de Minister van Justitie met betrekking tot rechtspersonen. De minister van Justitie heeft immers ingevolge Boek 2 BW slechts een wettelijke taak tot antecedentenonderzoek. De voorgestelde opsporingsfunctie staat hier haaks op.

Werkgevers gaan bij de sollicitatieprocedure niet altijd zorgvuldig te werk. Dit bleek onder meer bij de screening van politiepersoneel. De Registratiekamer ontving regelmatig signalen uit de politiepraktijk dat politiefunctionarissen en hun omgeving stiekem gescreend worden.

Zo constateerde de Registratiekamer dat een screening naar een parkeercontroleur c.q. buitengewoon opsporingsambtenaar op een aantal onderdelen niet conform de Wet politieregisters (Wpolr) en de daarbij behorende uitvoeringsregelingen had plaatsgevonden. Niet alleen had het volledige onderzoek buiten medeweten van de betrokkene plaatsgevonden, maar ook werd bij het onderzoek geput uit politieregisters zonder dat hiervoor een toereikende grondslag bestond. Bovendien is op ontoereikende gronden tot een negatief oordeel over de integriteit van betrokkene gekomen. Ten slotte schoten de rechtswaarborgen bij de onderzoeken tekort, alleen al omdat betrokkene van het ingestelde onderzoek onkundig is gebleven.

Naar aanleiding van de ontvangen signalen uit de politiepraktijk heeft de Registratiekamer de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) bij herhaling opgeroepen ervoor te zorgen dat deze onrechtmatige screeningspraktijken achterwege worden gelaten. Hoewel de Registratiekamer in bepaalde gevallen de noodzaak van dergelijke onderzoeken onderschrijft, stelt zij zich op het standpunt dat de uitvoering van deze onderzoeken met inachtneming van de hiervoor gestelde wettelijke kaders dient plaats te vinden: via de

verklaring omtrent het gedrag of door middel van een veiligheidsonderzoek. De politie moet volgens het huidige wettelijke kader de te screenen sollicitant of medewerker vertellen dat hen een onderzoek te wachten staat, hoe dat onderzoek wordt uitgevoerd en wie erbij worden betrokken. Ook moet de politie de uitkomsten meedelen. Aan stiekeme onderzoeken door de politie naar met name relaties van (toekomstig) politiepersoneel dient volgens de Registratiekamer snel een einde te komen.

De minister van BZK heeft instemmend gereageerd. Hij heeft in een brief van 22 oktober 1999 de Tweede Kamer als beleidslijn aangekondigd dat het aantal vertrouwensfuncties op grond van de Wet veiligheidsonderzoeken bij de politie zal worden uitgebreid. Verder heeft de minister de politie nogmaals gewezen op de wettelijke screeningskaders en erop aangedrongen dat andere vormen van screening worden beëindigd. De Registratiekamer heeft met instemming kennisgenomen van de nieuwe screeningsregels voor politiepersoneel.

In mei 1999 kwam het consumentenprogramma Radar met een uitzending over de schending van de privacy van een onderzochte persoon door een handelsinformatiebureau. In dit televisieprogramma werd aangetoond dat dit bedrijf een groot aantal gedetailleerde strafrechtelijke, financiële, arbeidsrechtelijke en medische gegevens buiten medeweten van betrokkene uit met name overheidsregistraties had vergaard. Deze uitzending leidde tot meerdere Kamervragen. De Registratiekamer heeft vervolgens een onderzoek ingesteld naar de wijze waarop door dit handelsinformatiebureau persoonsgegevens worden verzameld en vastgelegd. Uit het onderzoek van de Registratiekamer is gebleken dat op onrechtmatige wijze gegevens zijn verstrekt uit persoonsregistraties waarvoor een strikte geheimhoudingsplicht geldt. Het gebruik van de verkregen gegevens is onrechtmatig nu het voor het bureau duidelijk had moeten zijn dat deze privacygevoelige gegevens in strijd met de hiervoor geldende regels zijn verstrekt. Door deze gegevens vervolgens aan te wenden voor de rapportage heeft dit bureau dan ook onrechtmatig jegens betrokkene gehandeld. De Registratiekamer heeft het Ministerie van Justitie op de hoogte gesteld van de uitkomsten van dit onderzoek.

De toekomst van screening

De verwachting is gerechtvaardigd dat screening op integriteit ook de komende jaren hoog op de agenda van de overheid en het bedrijfsleven blijft staan. De Registratiekamer zal de ontwikkeling van de daarvoor benodigde instrumenten nauwlettend en kritisch volgen.

De minst ingrijpende methoden verdienen daarbij om diverse redenen de voorkeur. Veelal kan de betrokkene die aan screening op integriteit wordt onderworpen, als eerste bron fungeren. Zelfrapportage met verificatiemogelijkheden is immers een goed uitgangspunt. Van belang is dat goede criteria en procedures worden ontwikkeld voor (rechts)personen die aan screening worden onderworpen. Heldere informatie hierover aan de betrokkene is onmisbaar. Waar nodig dienen integriteitscriteria in sectorale wetten te worden opgenomen. Indien gebruik moet worden gemaakt van gesloten bronnen van de overheid dient de wetgever onder ogen te zien of en onder welke omstandigheden daarvan gebruik kan worden gemaakt. Het gaat in de praktijk hierbij met name om de registraties van politie en justitie.

Het bedrijfsleven vraagt zich af waarom de overheid de wettelijke instrumenten voor zichzelf reserveert. Het Nationaal Platform Criminaliteitsbeheersing heeft daarom uitwisseling van informatie met de overheid hoog op de agenda gezet. De regering zal zich op korte termijn dienen uit te laten over het door het bedrijfsleven uitgesproken verlangen.

Tijdens de consultatieronde heeft de Registratiekamer ernstige bedenkingen geuit tegen de voorgestelde BIBOB-regeling. Kort samengevat komt deze kritiek erop neer dat BIBOB mank gaat aan een gebrek aan evenwicht tussen het reële belang van een integere besluitvorming door het openbaar bestuur en de hiervoor noodzakelijk geachte inbreuken op de persoonlijke levenssfeer van de betrokkenen. In het wetsvoorstel ontbreekt een gedegen en overtuigende onderbouwing waarom een nieuw onderzoeksinstituut in het leven moet worden geroepen en waarom niet kan worden volstaan met bestaande en op stapel staande wetgeving. Het is minder ingrijpend – en dus beter – enkele sectorale wetten aan te passen. Om dezelfde reden kan volstaan worden met aanpassing van de Wpolr en de WJD teneinde het openbaar bestuur alsnog selectief toegang te geven tot strafrechtelijke informatie voor integriteitsbevorderende doeleinden.

Naast een kritische publicatie door twee medewerkers van de Registratiekamer in het Nederlands Juristenblad heeft de Registratiekamer bij vele gelegenheden deze kritiek herhaald. Tijdens deze gelegenheden bleek onder meer dat zowel het bedrijfsleven als de wetenschap de bezwaren van de Registratiekamer in grote lijnen delen. Deze kritiek heeft echter vooralsnog niet geleid tot aanpassing van het wetsvoorstel. Bij deze stand van zaken handhaaft de Registratiekamer haar bezwaren tegen BIBOB. De Registratiekamer besteedt om deze reden in 2000 in het bijzonder aandacht aan de parlementaire behandeling van de Wet BIBOB en volgt de belangrijkste lokale initiatieven ten aanzien van screening. De totstandkoming van de gewijzigde WJD acht zij van groot belang.

De Registratiekamer heeft begrip voor de groeiende behoefte bij overheid en bedrijfsleven om onder meer door screening het eigen integer handelen te waarborgen. De mogelijkheden moeten echter niet worden overschat. Screening is en blijft ook een ingrijpende inbreuk op de privacy van de betrokkenen. Essentieel is derhalve dat dit instrument wordt ingezet op een wijze die een adequaat niveau van bescherming van persoonsgegevens garandeert. Het in dit hoofdstuk beschreven toetsingskader zal voor de Registratiekamer hierbij de meetlat zijn.

Communicatie

Doeltreffend toezicht houden op de bescherming van de persoonlijke levenssfeer vergt een veelzijdige aanpak. Daarom heeft de Registratiekamer gekozen voor een 'viersporenbeleid', waarvan het eerste spoor gericht is op voorlichting en bewustwording. Dit omdat privacywetgeving alleen niet voldoende is. Het publiek moet natuurlijk weten dat er privacywetgeving is en wat deze betekent. Door effectieve communicatie wordt het belang van een zorgvuldig gebruik van persoonsgegevens voor steeds meer partijen duidelijk. De Registratiekamer gebruikt sinds 1999 ook een eigen website voor haar communicatie. Hoewel de Registratiekamer er nadrukkelijk voor kiest om niet alleen op incidenten en individuele zaken te reageren, kan het publiek natuurlijk wel gebruik maken van de expertise die bij de medewerkers van de Registratiekamer aanwezig is. Daarvoor heeft de Registratiekamer speciaal een front office opgericht dat publieksvragen snel en accuraat beantwoordt. Daarnaast organiseert de Registratiekamer bijeenkomsten en verzorgen medewerkers lezingen en artikelen in vakbladen. Ook journalisten benaderen de Registratiekamer wanneer zij op zoek zijn naar meer achtergrondinformatie of om te vragen naar een standpunt van de Registratiekamer. Daarnaast doet de Registratiekamer onderzoek naar nieuwe vraagstukken op het gebied van privacybescherming. De uitkomsten van zo'n onderzoek worden vaak in eigen beheer gepubliceerd.

www.registratiekamer.nl

Een belangrijke verbetering in 1999 was de ontwikkeling en lancering van de eigen website op het internet. Deze bevat onder andere informatie over actuele ontwikkelingen. Op de website zijn publicaties en uitspraken met behulp van een zoekmachine eenvoudig te vinden. Daarnaast staan op de site antwoorden op veel gestelde vragen. Ook is het mogelijk om voorlichtingsmateriaal te bestellen. Door langs deze weg te communiceren zijn verschillende doelgroepen sneller en beter bediend. In het verslagjaar brachten zo'n 25.000 internetgebruikers een bezoek aan de site. In 2000 zal de website van de Registratiekamer verder gevuld worden waardoor deze ook als archief geraadpleegd kan worden.

Frontoffice

Naast haar functie als tweedelijns-voorziening blijft de Registratiekamer natuurlijk bereikbaar voor het publiek. Door een uitbreiding van het frontoffice kan de Registratiekamer vragen en klachten van het publiek op een snelle en klantvriendelijke manier beantwoorden. Medewerkers van het frontoffice beantwoordden in het verslagjaar dagelijks enkele tientallen telefonische vragen. Ook beantwoordde het frontoffice zo'n 500 brieven en e-mail-berichten waarin vragen werden voorgelegd. Dit jaar waren er veel vragen over het controleren van e-mail- en internetgebruik door werkgevers. Deze vragen werden niet alleen gesteld door leden van Ondernemingsraden en systeembeheerders, maar ook door werkgevers. Begin 2000 hoopt de Registratiekamer met vuistregels te komen. Daarnaast waren er veel vragen over 'credit scoring.' Dit is het controleren van iemands betaalkracht bij het aangaan van een overeenkomst op krediet. Vaak ging het dan om een controle bij de aanschaf van een mobiele telefoon. Om deze vragen te beantwoorden heeft de Registratiekamer in mei 1999 het informatieblad *Het toetsen van uw kredietwaardigheid* uitgebracht. In 2000 zal tevens een rapport van de Registratiekamer over dit onderwerp verschijnen.

Lezingen en bijeenkomsten

Naast individuele vragen ontving de Registratiekamer verzoeken om gastcolleges, spreekbeurten of workshops te verzorgen voor groepen geïnteresseerden. Zo bezochten medewerkers van de Registratiekamer diverse scholen en universiteiten, dienstverlenende

instellingen en andere organisaties. Zij waren ook aanwezig bij verschillende vakbeurzen. Bijzonder nuttig en leerzaam was de aanwezigheid tijdens de Direct Marketing beurs in Maastricht. Juist binnen de direct marketing sector is het zorgvuldig omgaan met persoonsgegevens een kwaliteitsvoorwaarde. De Registratiekamer verheugde zich daarom in de grote belangstelling vanuit deze branche voor haar stand tijdens de beurs. Ook was de Registratiekamer aanwezig tijdens de Infosecuritybeurs in Utrecht.

De Registratiekamer bezocht niet alleen bijeenkomsten, maar organiseerde deze ook zelf om overleg te voeren met belanghebbende partijen. In juni organiseerde de Registratiekamer in samenwerking met het Nationaal Platform Criminaliteitsbeheersing een rondetafelconferentie over screening in Nederland. Tevens startte de Registratiekamer een samenwerkingsproject met koepelorganisaties en marktpartijen op het gebied van auditing, om te komen tot een gemeenschappelijke aanpak van privacy audits. Dit project wordt in 2000 afgerond.

Artikelen

In het tweemaandelijks tijdschrift *Privacy & Informatie* verzorgde de Registratiekamer in 1999 een katern waarin samenvattingen zijn opgenomen van de belangrijkste uitspraken en adviezen aan de regering. In het katern staat tevens een overzicht van recent verschenen publicaties. Met dit katern bedient de Registratiekamer met name beroepsmatig geïnteresseerden die op met behulp van dit katern een volledig actueel overzicht in handen krijgen.

Ook verzorgden leden en medewerkers van de Registratiekamer diverse artikelen in vakbladen en tijdschriften. Zo bracht de voorzitter een preadvies uit over de toepassing van Informatie Technologie in de gezondheidszorg voor de jaarvergadering van de Vereniging voor Gezondheidsrecht. Ook verscheen een artikel over de mogelijke gevolgen van de te late invoering van de Wet Bescherming Persoonsgegevens. In dit artikel werd wederom aangedrongen op een snelle aanpassing van de nationale wetgeving om ervoor te zorgen dat Nederland niet achterraakt bij de overige lidstaten. Een volledig overzicht van de gepubliceerde artikelen vindt u in bijlage 4.

Media

De mediavorlichting diende ook in 1999 als een belangrijk instrument om het brede publiek en specifieke doelgroepen te informeren over de standpunten en activiteiten van de Registratiekamer en de aandacht te vestigen op belangrijke ontwikkelingen. Gedurende het verslagjaar is de Registratiekamer zich meer bewust geworden van de gevoeligheid van de maatschappij voor publiciteit. Dit heeft ertoe geleid dat de woordvoering minder ingaat op incidenten, minder reageert en meer informeert.

Naast het dagelijks telefonisch contact met vooral de schrijvende pers, werkte de Registratiekamer ook in dit verslagjaar mee aan verschillende televisie-uitzendingen. Vooral een item in het TROS consumentenprogramma RADAR deed veel stof opwaaien. In dit programma werden de praktijken van een handelsinformatiebureau aan de orde gesteld. Dit leidde uiteindelijk tot kamervragen van diverse fracties en een onderzoek door de Registratiekamer. Uit het onderzoek bleek dat op onrechtmatige wijze gegevens waren verstrekt door instanties waar een geheimhoudingsplicht geldt.

Publicaties in eigen beheer

In 1999 deed de Registratiekamer onderzoek naar diverse ontwikkelingen. Over deze onderzoeken zijn publicaties in eigen beheer uitgebracht. De Registratiekamer doet dit onder

andere om aandacht te vragen voor nieuwe ontwikkelingen waarbij de bescherming van persoonsgegevens in het geding is en om haar positie als gesprekspartner te verstevigen. Zo verscheen in juli 1999 het rapport *Koning klant*, over het gebruik van klantgegevens voor marketingdoeleinden. In diezelfde maand verscheen eveneens het rapport *Werken met gegevens*. In het rapport werden vuistregels gepresenteerd voor de bescherming van persoonsgegevens bij gegevensuitwisseling tussen Centra voor Werk en Inkomen en uitzendbureaus.

In oktober 1999 verscheen *At face value* over biometrische identificatie. Hierbij wordt met behulp van een analyse van lichamelijke kenmerken zoals, stem, vingerafdruk, netvlies of iris vastgesteld dat iemand is wie hij of zij claimt te zijn. De Registratiekamer onderkende in dit rapport voordelen van

deze nieuwe techniek, omdat systemen met behulp van biometrie beter beveiligd kunnen worden. Tegelijkertijd plaatste de Registratiekamer kanttekeningen bij deze ontwikkeling. Zo werd onder andere gewezen op de gevaren van het centraal opslaan van gegevens. Het rapport *At face value* overhandigde de voorzitter van de Registratiekamer tijdens een persconferentie aan een geïnteresseerde minister van Boxtel van grote stedenbeleid, ook verantwoordelijk voor overheidsinformatiebeleid.

In het verslagjaar verscheen tevens de uitsprakenbundel *Persoonsgegevens beschermd*. In deze bundel staat een selectie van uitspraken en adviezen waarin de normen en regels van de huidige en toekomstige wetgeving, in specifieke situaties worden toegepast. Een volledig overzicht van de door de Registratiekamer uitgebrachte publicaties vindt u in bijlage 4.

Ontwikkeling van normen

De Registratiekamer draagt bij aan de ontwikkeling van nieuwe en concretisering van bestaande normen die de persoonlijke levensfeer beschermen tegen inbreuken op de verwerking van persoonsgegevens. In de tien jaar van haar bestaan is gebleken dat aan deze normontwikkeling een groeiende behoefte bestaat. Hiervoor zijn verschillende verklaringen te geven. De Wet persoonsregistraties (WPR) bevat diverse open en abstracte normen waarvan de concrete toepassing pas uit de praktijk blijkt. Dit wordt door critici van de wet vaak als bezwaar tegen de ‘privacywetgeving’ aangevoerd. Maar in dit opzicht verschilt de WPR niet van open normstellingen die ook andere belangrijke delen van het recht kenmerken. Zo ligt aan de uitvoering van het verbintenissenrecht het open beginsel van redelijkheid en billijkheid

als maatstaf ten grondslag. Abstracte bepalingen als zorgvuldigheid en belangenafweging kenmerken het algemeen bestuursrecht. De wetgeving voor de omgang met persoonsgegevens bevat specifieke maatstaven aan de hand waarvan nadere invulling van de open normen dient te geschieden. Deze zijn in veel gevallen op internationale verdragen gebaseerd. Met het verbintenissenrecht heeft deze wetgeving gemeen dat zij betrekking heeft op veel en uiteenlopende sectoren van de maatschappij. Anders dan het civiele recht is deze vorm van 'privacyrecht' echter nieuw en in de rechtspraak nog weinig uitgekristalliseerd.

Het voorgaande vormt een verklaring voor de stroom van vragen die op diverse manieren op de Registratiekamer afkomen en die veelal betrekking hebben op de gewenste specificatie van de normen naar de concrete situatie van de vraagsteller. Vraagstellers zijn zowel individuele burgers - als consument, werknemer, patiënt, verdachte - als organisaties, bedrijven en overheidsinstellingen.

Als toezichthouder op de WPR en verwante wetgeving rekent de Registratiekamer het bijdragen aan de normontwikkeling dan ook tot één van haar belangrijkste taken. Zij bedient hierbij verschillende doelgroepen en doet dit op verschillende manieren. In de opzet van dit jaarverslag past geen integraal overzicht van de werkzaamheden op het gebied van normontwikkeling. Volstaan wordt met een globale aanduiding van deze werkzaamheden en het belichten van enkele voor de normontwikkeling relevante publicaties en zaken. De beschrijving verloopt van activiteiten met een algemene strekking naar specifieke bijdragen aan de normontwikkeling.

Publieksvoorlichting over normen

Het werken aan bewustwording over de omgang met persoonsgegevens gebeurt met name door het in brede kring bevorderen van het privacybesef. Dit geschiedt door het vertalen van de abstracties van dit recht naar concrete werkterreinen. Een werkwijze hiervoor is de vertaling van veel voorkomende vragen die met name bij onze telefonische helpdesk binnenkomen, naar informatiebladen die op brede schaal worden verspreid. Deze staan sinds vorig jaar overigens ook op de internetsite van de Registratiekamer (www.registratiekamer.nl).

In de voorlichting over normen past de publicatie van de tweede druk van de uitgave *Persoonsgegevens beschermd: van WPR naar WBP*. Het gaat om een bundeling van uitspraken van de Registratiekamer over de eerste tien jaar van haar bestaan. Bij de selectie is rekening gehouden met de aanstaande invoering van de Wet bescherming persoonsgegevens (WBP). De interpretatie van de normen uit de WPR blijft echter van belang. De WBP bouwt immers – zeker voor wat betreft de materiële normen – voort op het onder de WPR ontwikkelde kader. Van de actuele normontwikkeling kan worden kennis genomen door raadpleging van de (samenvattingen van) relevante uitspraken op de internetsite van de Registratiekamer.

Wetgevingsadviezen

Onder de WBP zullen - evenals onder de WPR - voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens, om advies aan de Registratiekamer moeten worden voorgelegd. Dit betekent een systematische betrokkenheid bij de normontwikkeling op dit niveau, zowel in het kader van de WBP als daarbuiten. In 1999 bracht de Registratiekamer over 27 wetsontwerpen dan wel ontwerpen van algemene maatregelen van bestuur advies uit. De informatiehuishouding bij de uitvoering van belangrijke overheidstaken stond op diverse

manieren op de agenda van de Registratiekamer. Achtereenvolgens betrof het de herinrichting van de sociale zekerheid, de plannen voor vereenvoudiging van het stelsel van individuele huursubsidie, het gebruik van het sofi-nummer en de ongebreidelde groei van informatieverstrekking via de fiscus.

Herinrichting sociale zekerheid

In 1999 vond de parlementaire discussie plaats over het standpunt van het kabinet over de nieuwe uitvoeringsstructuur in de sociale zekerheid in de nota Structuur Uitvoering Werk en Inkomen (SUWI I). Tijdens de hoorzitting op 14 juni in de Tweede Kamer vroeg de Registratiekamer aandacht voor het belang dat binnen de nieuwe uitvoeringsstructuur specifieke regels opgesteld worden voor de verwerking van persoonsgegevens. Persoonsgegevens van (aspirant) uitkeringsgerechtigden/verzekerden vormen hier immers het belangrijkste bedrijfskapitaal. Informatiestromen moeten voldoende inzichtelijk zijn. De handhaving van de regels moet in de informatiesystemen geborgd zijn. De Registratiekamer achtte specifieke regelgeving dan ook onmisbaar: burgers zijn nu eenmaal verplicht hun gegevens aan de uitvoeringsinstellingen te verstrekken. Daar komt bij dat de gegevens vaak gevoelig van aard zijn: ziektegeschiedenis, sociale omstandigheden en financiële gegevens. Bovendien staan voor betrokkenen zeer grote belangen op het spel, het gaat om hun bestaanszekerheid.

Uitgangspunt dient te zijn dat persoonsgegevens slechts mogen worden gebruikt voor de doeleinden waarvoor ze zijn verzameld: de uitvoering van de sociale zekerheid. Voor verder gebruik van de gegevens geldt de toets van de verenigbaarheid met het oorspronkelijke doel. In de visie van de Registratiekamer is verdergaand gebruik van de persoonsgegevens niet uitgesloten: bijvoorbeeld voor een aanvullende particuliere verzekering van het WAO-hiaat. De toetsing op grond van verenigbaar gebruik biedt op dit terrein te weinig rechtsbescherming voor de verzekerde. Specifieke wetgeving is dan ook onmisbaar.

In het algemeen acht de Registratiekamer toestemming van de verzekerde een ontoereikende grondslag om de nieuwe informatiehuishouding in de sociale zekerheid op te baseren. Toestemming van betrokkenen voor verder gebruik van hun gegevens kan alleen een geldige grondslag zijn als deze vrijwillig wordt gegeven. Gelet op diens verplichting om gegevens te verstrekken en de afhankelijke positie van betrokkenen is daarvan niet snel sprake. Overigens kan de toestemming steeds worden ingetrokken. Daarmee is toestemming geen behoorlijke en ook geen solide basis voor systematisch gebruik van persoonsgegevens.

In de sterk bijgestelde plannen van de regering SUWI II wordt de uitvoering van de sociale verzekeringen geconcentreerd in een publiekrechtelijke organisatie. Deze concentratie betekent een aanmerkelijke beperking van het gegevensverkeer en komt daarmee de bescherming van persoonsgegevens ten goede. Wel heeft de Registratiekamer voor twee aspecten in het bijzonder aandacht gevraagd: de gegevensuitwisseling bij reïntegratie van zieke, arbeidsongeschikte en werkloze werknemers en de gegevensuitwisseling bij aanvullende verzekeringen. De Registratiekamer acht een kaderwet noodzakelijk waarin deze punten voor de sociale zekerheidssector worden geregeld. Tussen betrokken partijen kunnen aanvullend protocollen worden opgesteld met betrekking tot de onderlinge gegevensuitwisseling.

Vereenvoudiging van het stelsel van individuele huursubsidie

Het ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer (VROM) gaat in het kader van de Huursubsidiewet (Hsw) persoonsgegevens uitwisselen met de

belastingdienst, de bevolkingsadministratie (GBA), gemeenten en de verhuurder. De huurder dient een aanvraag in en VROM vraagt de noodzakelijke gegevens op bij de belastingdienst, de GBA en de verhuurders. Op basis van de huur-, inkomens- en bewoningsgegevens van alle leden van het huishouden wordt de subsidie vastgesteld.

De huursubsidie kan worden gecontinueerd zonder dat daartoe een vervolgaanvraagformulier hoeft te worden ingediend. VROM vraagt de gegevens op bij de belastingdienst en de verhuurder voor het continueren van de huursubsidie. Indien inmiddels iemand is komen in te wonen op een huursubsidieadres, wordt dit automatisch via een melding uit de GBA doorgegeven aan VROM. Het ministerie neemt dan contact op met de belastingdienst voor inkomensgegevens van de medebewoner. De aanvrager krijgt de gegevens ter verificatie toegestuurd.

De Registratiekamer adviseerde voor het nieuwe systeem een wettelijke regeling te ontwerpen in plaats van te kiezen voor een stelsel waarin toestemming van de betrokkenen wordt gevraagd. Een wettelijke regeling doet recht aan het karakter van de individuele huursubsidie en aan de positie van de aanvrager en diens medebewoners. Bij een inkomensafhankelijke overheidsregeling als deze past het immers dat de uitvoerende instantie verifieert of de aanvrager recht heeft op die regeling. Aan deze procedure heeft de aanvrager zich nu eenmaal te onderwerpen. Wel dient hij ook over deze verificatie tevoren goed te worden geïnformeerd.

De gegevensuitwisseling moet zo specifiek mogelijk worden aangeduid. Juist gelet op de grootschalige toepassing van de Hsw – 800.000 huishoudens – is dit een sleutelement van een adequate privacybescherming. Niet kan worden volstaan met een globale aanduiding als ‘de uitwisseling van gegevens is noodzakelijk voor de uitvoering’. De aard dient nauwkeurig te worden omschreven en de noodzaak hiervan dient toereikend te worden onderbouwd. Verder dient de kring van personen op wie deze uitwisseling ingevolge de Hsw betrekking mag hebben, te worden gespecificeerd. In het algemeen geldt dat de standaardset van gegevens die nodig is voor de verificatie en toekenning van de subsidie in beginsel de bovengrens aan de uitwisseling van gegevens vormt.

Een goede invulling van het transparantiebeginsel is cruciaal. Derden, zoals huisgenoten, hoeven er immers niet van op de hoogte te zijn dat hun gegevens bij het proces van verificatie van gegevens betrokken worden. Voordat derden in het beoordelingsproces worden betrokken moet op deugdelijke wijze vastgesteld te worden dat hun gegevens voor het beoordelen van de aanvraag voor individuele huursubsidie relevant zijn.

VROM heeft het advies van de Registratiekamer in belangrijke mate opgevolgd in het later dit jaar aan haar voorgelegde wetsvoorstel. De Registratiekamer adviseerde ook over dit voorstel en vroeg met name aandacht voor de noodzaak om de set van gegevens die nodig was voor de vaststelling van de huursubsidie, specifiek te omschrijven.

Het gebruik van het sofi-nummer

Twee adviezen uit 1999 gingen over het gebruik van het sofi-nummer, dat is opgezet voor gebruik in bepaalde sectoren, met name voor de belastingheffing en de sociale zekerheidswetgeving. Het nummer heeft in dat kader ook een functie gekregen bij bestrijding van fraude en van andere criminaliteit. De risico's van het gebruik van het sofi-nummer nemen toe en dreigen onbeheersbaar te worden naarmate het nummer op ruimere schaal wordt verspreid. De Registratiekamer toetst de rechtmatigheid van het gebruik telkens aan het domein waarvoor dit nummer is ontworpen en het geldende wettelijk kader. Het sofi-nummer

wordt toegekend door de belastingdienst en is een uniek en verplicht persoonsnummer voor elke burger die gebruik maakt van of valt onder een fiscale of sociale zekerheidswetgeving. Het sofi-nummer is, naast de genoemde wetgeving, slechts voor de uitvoering van bepaalde andere wettelijke voorschriften toegestaan.

Passend binnen het Sofi-domein is het gebruik van het sofi-nummer in de administratie van de uitvoeringsorganen van de Algemene wet bijzondere ziektekosten (AWBZ) invoeren. De regering wilde hiermee de invoering van het sofi-nummer in de sociale verzekeringswetten voltooien. De Registratiekamer kwam dan ook tot een positief advies over het betrokken wetsvoorstel. Zij wees daarbij wel op het belang een onderscheid aan te brengen tussen informatie voor de zorgkant enerzijds en voor de financieringskant anderzijds. Het sofi-nummer mag in de AWBZ alleen gebruikt worden voor de financiële afwikkeling van declaraties.

De minister van Justitie vroeg om advies over een wijziging van het Wetboek van Strafvordering, op grond waarvan de politie bevoegd zou worden een verdachte naar diens sofi-nummer te vragen. Aan de hand hiervan kan de politie de identiteit bij de gemeentelijke basis administratie verifiëren. Daar dit neer zou komen op een uitbreiding van het Sofi-domein adviseerde de Registratiekamer negatief. De minister van Justitie handhaafde zijn voorstel, maar perkte het gebruik uitdrukkelijk in tot de verificatie. Hierdoor wordt voorkomen dat het Sofi-nummer als sectoraal nummer in de strafrechtsketen wordt ingevoerd.

Informatieverstrekking via de fiscus

De minister van Sociale Zaken en Werkgelegenheid heeft het advies van de Registratiekamer opgevolgd om banken niet te verplichten cliëntgegevens direct te laten verstrekken aan sociale diensten. Het voornemen van de minister om bij Algemene Maatregel van Bestuur (AMvB) de banken aan te wijzen als informatieplichtig hield in dat banken door tussenkomst van de belastingdienst rentegegevens en rekeningnummers van hun cliënten zouden moeten verstrekken aan sociale diensten.

De Registratiekamer achtte de voorgestelde informatieverplichting dubieus en onwenselijk. Een verplichting tot gegevensverstrekking die het recht op eerbiediging van de persoonlijke levenssfeer beperkt, is slechts mogelijk bij of krachtens een wet in formele zin en dient te voldoen aan de criteria die het Europees verdrag voor de rechten van de mens en de fundamentele vrijheden stelt. Zo zal het voorschrift voldoende nauwkeurig moeten zijn omschreven en adequate en effectieve waarborgen moeten bevatten tegen ongeoorloofde inbreuken. Dit betekent dat de beperking moet worden gerechtvaardigd door een “pressing social need” en in overeenstemming moet zijn met de beginselen van proportionaliteit (de beperking van het recht op privacy mag niet onevenredig zijn in verhouding tot het nageleefde doel) en subsidiariteit (het nageleefde doel mag niet op een voor de burger minder ingrijpende manier worden bereikt). Het concept AMvB voldeed niet aan deze vereisten. Een klemmende vraag was waarom er niet kan worden volstaan met de huidige regelingen en mogelijkheden van sociale diensten om gegevens te controleren.

Over de gekozen constructie, gegevensverstrekking door banken met tussenkomst van de belastingdienst, heeft de Registratiekamer opgemerkt dat de belastingdienst al verplicht is persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van deze wet. Er zijn geen formele beletselen om naast de gegevens die nu reeds verstrekt worden, ook gegevens over het vermogen te verstrekken. De belastingdienst verkrijgt die gegevens van de banken via het Voorschrift Informatie Fiscaal/banken. De Registratiekamer heeft ernstige

bezwaren tegen de voorgestelde ondoorzichtige en juridisch dubieuze constructie. In de huidige praktijk geeft de belastingdienst informatie door die deze ten behoeve van de eigen taakuitoefening heeft vergaard. Hiertoe zullen ook de onderhavige gegevens over bankrekeningnummers en rente-inkomsten behoren. Het bij AMvB bepalen dat de belastingdienst als doorgeefluik van informatie aan andere instanties dient, schept echter een precedent waarbij de Registratiekamer vraagtekens plaatst.

Gedragscodes

Bij de concretisering en nadere invulling van de wettelijke normen voor de verwerking van persoonsgegevens is in de WPR een grote plaats ingeruimd voor zelfregulering in de vorm van gedragscodes voor bepaalde sectoren. De Registratiekamer heeft de taak om de totstandkoming van deze gedragscodes te stimuleren en de kwaliteit ervan in het kader van een vrijwillige goedkeuringsprocedure te toetsen. De betrokken regeling zal in de WBP behoudens aanpassing op onderdelen, zoals de invoering van rechtsbescherming tegen het uitblijven van goedkeuring, worden gehandhaafd. Ook in de toekomst zal zelfregulering dus een belangrijke rol kunnen spelen bij de implementatie van de WBP.

In het verslagjaar zijn ter voorbereiding op de invoering van de WBP met diverse organisaties besprekingen gevoerd om te komen tot de invoering van een gedragscode onder deze wet. De Registratiekamer bevordert de totstandkoming van dergelijke codes.

Aan de vergadering van de toezichthouders binnen de Europese unie, de groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens zijn twee ontwerpgedragscodes voorgelegd. Na goedkeuring zullen deze werking hebben voor de gehele Europese unie. Het gaat om een code voor de direct marketing branche, ingebracht door de Europese brancheorganisatie FEDMA, en een ontwerpcode van de internationale luchtvaartmaatschappijen verenigd in de IATA.

Ontwerpen normatieve kaders

De Registratiekamer signaleert regelmatig dat op bepaalde maatschappelijke terreinen of voor bepaalde onderwerpen behoefte bestaat aan kaders voor een zorgvuldige omgang met persoonsgegevens. Op diverse wijzen voorziet zij in deze behoefte. In de meest eenvoudige vorm wordt het publiek bediend met informatiebladen. Fundamenteeler behandelt zij onderwerpen in de serie Achtergrondstudie en Verkenningen (A&V). In deze reeks verschenen onder meer richtlijnen voor de aanleg van zwarte lijsten (A&V-studie nr. 4, 1995) en cliëntvolgsystemen (*Doelbewust volgen*, A&V-studie nr. 9, 1998). Ook in andere publicaties geeft de Registratiekamer invulling aan de voor een specifiek onderwerp relevante privacyregels. De meest gevraagde uitgave is *In beeld gebracht* (Privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging, 1997). De hierin vervatte regels zijn ook in 1999 voor diverse projecten op het gebied van videocamerabewaking als uitgangspunt gehanteerd. De uitgave ligt ook ten grondslag aan de wetgeving die thans door de minister van Justitie en Binnenlandse Zaken en Koninkrijksrelaties wordt voorbereid.

In 1999 besteedde de Registratiekamer aandacht aan de verwerking van klantgegevens, de informatieverstrekking door de belastingdienst, de samenwerking bij de uitvoering van de sociale zekerheid met uitzendbureaus en de stand van privacybescherming bij de sociale diensten.

Koning klant: de verwerking van klantgegevens

De Registratiekamer constateerde dat in de praktijk behoefte bestond aan duidelijkheid over het gebruik dat bedrijven mogen maken van hun klantgegevens. Bedrijven leggen steeds vaker klantgegevens vast. Hierdoor kunnen deze bedrijven nauwkeurig in kaart brengen wie hun (potentiële) klanten zijn en daarop hun verkoop- en/of reclamestrategie afstemmen. Het is technisch goed mogelijk om grote aantallen gegevens in databases vast te leggen, terwijl het relatief eenvoudig is om deze gegevens via analyse te herleiden tot waardevolle (tot personen herleidbare) informatie. Daardoor wordt op steeds grotere schaal gebruik gemaakt van deze mogelijkheden. Welk gebruik is toegestaan is in de publicatie *Koning Klant* (A&V-studie nr. 14, juli 1999) getoetst aan de toekomstige Wet bescherming persoonsgegevens. De Registratiekamer behandelt hierin de meest voorkomende klantrelaties van koop op de markt tot deelname aan loyalty- of spaarprogramma's. Zij geeft daarbij telkens aan welke klantgegevens in de desbetreffende relatie van belang zijn en welk gebruik de aanbieder daarvan mag maken. De relatie tussen de aanbieder van producten en diensten en de klant bepaalt wanneer en op welke wijze het verwerken van klantgegevens voor marketingdoeleinden is toegestaan.

De aanbieder zal zich reeds bij de bouw van zijn klantenbestand moeten afvragen welke gegevens noodzakelijk zijn om het beoogde doel te kunnen realiseren. Hierbij is een terughoudende opstelling van de aanbieder vereist. Als de klantgegevens op een rechtmatige wijze in een klantenbestand zijn vastgelegd, kan de aanbieder hiervan in veel gevallen gebruik maken om de geregistreerde klanten persoonlijk te benaderen, ook zonder de toestemming van die klanten. Een dergelijk gebruik zal in het algemeen verenigbaar zijn met het doel waarvoor de gegevens zijn verzameld. Wel is vereist dat de klanten op de hoogte zijn van het gebruik van hun gegevens zodat zij hun rechten kunnen uitoefenen. Zo dient verzet van de klant tegen het gebruik van zijn gegevens voor direct marketing activiteiten altijd te worden gehonoreerd.

De informatieverstrekking door de belastingdienst

De Belastingdienst verstrekt steeds meer persoonsgegevens aan andere organisaties, zonder dat dat verband houdt met de uitvoering van de belastingwet. Het wettelijke uitgangspunt is dat de Belastingdienst verplicht is tot geheimhouding. De minister van Financiën kan echter ontheffing van die geheimhoudingsplicht verlenen. Aangezien van deze ontheffingsmogelijkheid steeds vaker gebruik wordt gemaakt, heeft de Registratiekamer erop gewezen dat dit een spanningsveld oplevert tussen geheimhouding enerzijds en de belangen bij het verstrekken van gegevens anderzijds. Tegen die achtergrond wordt geconcludeerd dat de toepasselijke wettelijke regeling voor de verstrekking van persoonsgegevens door de fiscus - in het licht van privacywetgeving - niet meer up-to-date is. Het belangrijkste probleem is het ontbreken van een adequate wettelijke grondslag met bijbehorende waarborgen. De Registratiekamer acht het gewenst dat daarin - in het verlengde van de op dit moment aanhangige herziening van het belastingrecht - wordt voorzien.

Deze conclusies zijn opgenomen in de publicatie *Informatieverstrekking door de fiscus - ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving* (A&V-studie nr. 16). De publicatie is aan staatssecretaris Vermeend van Financiën en de Tweede Kamer aangeboden. De staatssecretaris heeft toegezegd het wettelijke regime te wijzigen.

Belastingen is een bijzonder aandachtsgebied van de Registratiekamer. De Belastingdienst is als 'grootgebruiker' van gegevens over burgers en bedrijven verantwoordelijk voor de zorgvuldige verwerking van veel vertrouwelijke informatie. Gestreefd wordt naar een structurele verbetering van de bescherming van fiscale gegevens. In dat kader is de studie

uitgevoerd naar de garingsbevoegdheden van de fiscus die begin februari 1998 werd afgerond. De Registratiekamer wil door het uitvoeren van dergelijke studies bijdragen aan een structurele verbetering van de bescherming van fiscale gegevens.

De samenwerking bij de uitvoering van de sociale zekerheid met uitzendbureaus

In de toekomst zullen steeds meer Centra voor Werk en Inkomen (CWI's) worden opgericht. In de CWI's gaan arbeidsbureaus, uitvoeringsinstellingen en sociale diensten samenwerken om de uitkeringsgerechtigden aan het werk te helpen. De uitkeringsgerechtigde hoeft dan nog maar naar één loket te gaan. Hier wordt dan gekeken hoe hij aan het werk kan worden geholpen en welke instelling het recht op uitkering kan vaststellen. De CWI's schakelen soms derden in om hun taken uit te voeren of te helpen uitvoeren. Een van hun gezamenlijke taken is het aan het werk helpen van de uitkeringsgerechtigden. De uitkeringsgerechtigde is daarbij vaak verplicht zich in te zetten om aan werk te komen. De Registratiekamer constateerde dat bij de diverse deelnemers aan CWI's onzekerheid bestond over de mogelijkheden van uitwisseling van persoonsgegevens. Zij onderzocht hoe aan de samenwerking tussen CWI's en uitzendbureaus vormgegeven kan worden op een wijze die recht doet aan de privacyregels. Vervolgens heeft zij in samenspraak met de diverse partijen vuistregels opgesteld, waarbij rekening werd gehouden met de toekomstige Wet bescherming persoonsgegevens.

De stand van privacybescherming bij de sociale diensten

In 1997 vroeg de Registratiekamer met het rapport *Privacy en de Algemene bijstandswet* aandacht van de minister van Sociale Zaken en Werkgelegenheid en de gemeenten voor knelpunten in de privacybescherming bij de uitvoering van de - nieuwe - Algemene bijstandswet (Abw). De minister reageerde hierop in 1998 met het uitbrengen van een privacykader voor de uitvoering van de Abw. Vervolgens deed de Registratiekamer een dossieronderzoek bij drie sociale diensten naar de naleving van dit privacykader. Sociale diensten weten niet altijd welke gegevens noodzakelijk zijn om in bijstandsdossiers op te nemen. Veel sociale diensten hebben echter een verantwoorde werkwijze voor gegevensverkeer en een controleerbaar uitvoeringstraject. Dit zijn de belangrijkste conclusies uit dit onderzoek. Hoofddoel van het onderzoek was het opnemen van de stand van zaken van het verwerken van persoonsgegevens bij de uitvoering van de Abw. Op 9 februari 1999 werden de resultaten van het onderzoek kort gepresenteerd tijdens de themadag 'Privacy en de Algemene bijstandswet'.

Uit het onderzoek bleek dat een sociale dienst zelf zeer goed kan bepalen wat noodzakelijk is. Zij hebben een eigen verantwoordelijkheid hiervoor. De sociale dienst kan door eigen kennis en ervaringen komen tot een verantwoorde werkwijze bij het gegevensverkeer en een correct en controleerbaar uitvoeringstraject. Daarom is het zeer goed dat de onderzochte gemeenten een eigen privacybeleid hebben opgesteld. Zo kan een balans gevonden worden tussen de bescherming van de persoonsgegevens en de controle op de rechtmatigheid van de uitkering en controle op de uitvoering. Belangrijke aandachtspunten zijn dat uit de dossiers blijkt waar de gegevens vandaan komen en blijven en dat de cliënt weet wat er gebeurt op het gebied van categorisering, verificatie en het verstrekken van gegevens. Om gegevens te verkrijgen bij andere dan in de wet daartoe verplichte instanties is de toestemming van de cliënt nodig. Deze toestemming kan in een concrete situatie het beste met een apart formulier gevraagd worden.

Geschillen beslecht

Op het grensvlak van normontwikkeling en handhaving ligt de betrokkenheid van de Registratiekamer bij geschillen. Het kan gaan om de behandeling van klachten of verzoeken om bemiddeling. In een groeiend aantal gevallen vraagt de rechter de Registratiekamer te

adviseren over een aan hem voorgelegd geschil met betrekking tot inzage, correctie of verwijdering van persoonsgegevens. De afdoening van dergelijke geschillen kan aanleiding geven tot uitspraken waarin de normen van de wet nader worden uitgelegd en verduidelijkt. Een soortgelijke situatie kan zich voordoen bij verzoeken om voorlichting, hoewel het karakter daarvan doorgaans zal dwingen tot grote terughoudendheid. De situaties waarin een dergelijke uitspraak kan worden gedaan, zullen onder de WBP waarschijnlijk toenemen. Dit komt mede door nieuwe taken, zoals het voorafgaand onderzoek en het verlenen van een ontheffing voor de verwerking van bijzondere gegevens. Vaker dan thans zal echter ook beroep op de rechter openstaan, zodat deze kan beslissen over de juistheid van de eerder gegeven uitspraak.

Bij het bezien van de oogst aan relevante uitspraken over 1999 valt op dat diverse hiervan betrekking hebben op de (driehoeks)relatie werknemer/werkgever en verzekeringsmaatschappij. Juist in dergelijke relaties krijgt de bescherming van de persoonlijke levenssfeer reliëf. Een belangrijke kwestie betrof voorts het gebruik van medische gegevens door een zorgverzekeraar.

Privacy in arbeidsverhoudingen

Uit de diverse privacykwesties die op het terrein van de arbeidsverhoudingen speelden, zijn het onderzoek van e-mail van werknemers, de aanmelding van nevenfuncties, het uitwisselen van gegevens tussen een werkgever en een verzekeringsmaatschappij en de marketing met werknemersgegevens het vermelden waard.

Een computerbedrijf heeft als wereldwijd beleid dat de werkgever inzage kan eisen in de e-mail en voice mail berichten 'for any purpose' en stelt dat de werknemers 'no reasonable expectation of privacy' hebben wanneer zij e-mail of voicemail gebruiken. De Ondernemingsraad (OR) vraagt de Registratiekamer om een oordeel over dit beleid. Uitgangspunt voor haar beoordeling is dat bestanden waarin e-mail berichten zijn opgeslagen zijn aan te merken als persoonsregistraties in de zin van de Wet persoonsregistraties (WPR). Het standpunt van de werkgever dat hij voor 'for any purpose' e-mail berichten mag openen, gebruiken, kopiëren en verspreiden komt in strijd met de WPR. Hij zal een redelijk belang hiervoor moeten kunnen aantonen dat overeenkomt met het doel van de registratie met e-mailberichten. Ook diens opvatting dat de werknemer 'no reasonable expectation of privacy' hebben is in het licht van de privacywetgeving niet houdbaar.

De Registratiekamer beveelt aan dat voor gebruik en controle van e-mail duidelijke procedures worden opgesteld. Dit komt de transparantie van het informatieverwerkend proces ten goede. De werkgever zal de grenzen in acht moeten nemen: hoe verhoudt het doel dat de werkgever bij de registratie van gegevens voor ogen staat zich tot het belang van de werknemers? Kan het doel worden bereikt met andere middelen, die minder diep ingrijpen in de persoonlijke levenssfeer van de werknemers? Aan dit afwegingsproces kan de OR een bijdrage leveren door het uitoefenen van het instemmingsrecht.

Ook stelde de Registratiekamer een onderzoek in naar aanleiding van berichten in de media dat een multinationalaal bedrijf een aantal werknemers had ontslagen wegens verspreiding van pornografisch materiaal via het bedrijfscomputernetwerk. De aanleiding hiervoor was een klacht van een medewerker dat hij ongewenst e-mail had ontvangen met bijgevoegde pornografische filmpjes en plaatjes. Deze waren afkomstig van een afzender binnen het bedrijf. Vaststond dat de afzender door het versturen van dergelijke berichten het geldende

bedrijfsbeleid voor het gebruik van het bedrijfscomputernetwerk had overtreden. Dit beleid bepaalde dat het verboden was om onder meer online te gokken, kettingbrieven of pornografisch materiaal te versturen, discriminerende of seksueel intimiderende opmerkingen te maken of ander 'illegal' of 'harrassing' materiaal te verzenden. Het bedrijf hield zich het recht voor om alle mailberichten en het internetgebruik te onderzoeken zonder de betrokken medewerker daarvan op de hoogte te stellen. Dit beleid werd op het openingsscherm van het systeem aan de gebruiker medegedeeld.

Het onderzoek door het bedrijf had zich beperkt tot de mailboxen van de groep medewerkers die afzenders of ontvangers waren van de 'verboden' berichten. Op een peildatum waren alle berichten met een 'attachment' (een bijlage) geopend om vast te stellen of de bijlage een plaatje, filmpje of programma betrof. Berichten zonder attachment werden niet geopend tenzij uit de titel bleek dat het om pornografisch materiaal ging.

De Registratiekamer overwoog dat het tegengaan van misbruik van het bedrijfscomputernetwerk een gebruik is dat verenigbaar is met het voorschrift dat het systeem van e-mail vooral voor zakelijk gebruik was bestemd. Zij achtte het door het bedrijf verrichte onderzoek overigens behoorlijk en zorgvuldig, gelet op de wijze en de beperkte omvang waarop het bedrijf het onderzoek heeft uitgevoerd. Wel plaatste zij kanttekeningen bij de voorwaarden die door het bedrijf geformuleerd waren voor gebruik van het systeem. De bevoegdheid die het bedrijf zichzelf toekent om te allen tijde de berichten te controleren buiten medeweten van de medewerkers is in het algemeen te ruim om een inbreuk op de persoonlijke levenssfeer van de medewerkers te rechtvaardigen.

De ondernemingsraad van een penitentiaire inrichting vroeg de Registratiekamer of de door de minister van Justitie aan de justitieambtenaren opgelegde verplichting om nevenwerkzaamheden *te allen tijde* bij het bevoegd gezag te melden verder gaat dan waartoe het Algemeen Rijksambtenarenreglement (ARAR) verplicht. De minister van Justitie stelde hiertegenover dat een meldingsplicht voor *alle* nevenwerkzaamheden gerechtvaardigd is met het oog op het de specifieke justitietaak en het hoge (afbreuk)risico van een onjuiste afweging door de medewerker zelf.

Uit de totstandkoming van de desbetreffende bepaling uit het ARAR bleek dat uitgegaan moet worden van een beperkte meldingsplicht, waarbij de ambtenaar een zekere mate van zelfbeoordeling wordt gegeven omtrent de verplichting tot melding.

Registratie van gegevens die worden verkregen als gevolg van een te vergaande meldingsverplichting kan in strijd komen met de Wet persoonsregistraties (WPR). De nevenwerkzaamheden mogen in dat geval volgens de Registratiekamer niet worden opgenomen in het personeelsinformatiesysteem van justitie

De minister van Binnenlandse Zaken oordeelde desgevraagd dat het niet onbegrijpelijk was dat in departementale richtlijnen dringend wordt aanbevolen alle nevenfuncties te melden. Het achterwege laten daarvan brengt immers risico's van een verkeerde inschatting mee voor de ambtenaar. De Minister van Justitie ging echter verder dan een dringende aanbeveling. Zijn collega onderschreef het standpunt van de Registratiekamer dat daarmee de beperkte meldingsplicht van het ARAR en de registratiebevoegdheid van de WPR werd overschreden.

De minister van Justitie heeft naar aanleiding van deze uitspraak de circulaire op 30 december 1998 herzien. In de nieuwe versie staat nog slechts een dringende aanbeveling om alle nevenwerkzaamheden te melden.

Het uitwisselen van gegevens tussen een werkgever en een verzekeringsmaatschappij

De manier waarop de Algemene Nabestaandenwet de uitkering aan de nabestaanden regelt, kan een hiaat in hun inkomen tot gevolg hebben. Een bedrijf heeft voor zijn vaste werknemers collectief een voorlopige dekking van dit 'ANW-hiaat' afgesloten bij een verzekeringsmaatschappij. De verzekeraar heeft voor de definitieve verzekering aan de werkgever gevraagd om een algemene gezondheidsverklaring en een opgave van de werknemers die de laatste zes maanden wegens een ernstige ziekte onder medische behandeling zijn geweest of langer dan vier weken hebben verzuimd. Ook wil de verzekeraar weten welke werknemers arbeidsongeschikt zijn of AAW/WAO ontvangen, of van wie omstandigheden bekend zijn die tot verhoging van de kans op ziekte of arbeidsongeschiktheid kunnen leiden. Het bedrijf heeft zo'n verklaring, met de namen van langdurig zieken en WAO-ers aan de verzekeringsmaatschappij afgegeven. De aard van de ziekte en het afkeuringpercentage stonden bij de die namen vermeld. De individuele medewerkers hebben daarvoor geen toestemming gegeven. Aan de werknemers van wie de naam was doorgegeven, heeft de verzekeringsmaatschappij vervolgens gevraagd om een individuele gezondheidsverklaring af te geven. De Ondernemingsraad vroeg de Registratiekamer om een reactie.

Het uitgangspunt van de Registratiekamer was dat gegevens uit een personeels- of salarisadministratie, zoals over het ziekteverzuim aan een verzekeraar, verstrekt mogen worden als dat nodig is voor een voor de betrokkene geldende arbeidsvoorwaarde. Bij een gegevensverstrekking die verband houdt met het sluiten van een verzekering - waar juist die betrokkene met gezondheidsklachten wel eens van zou kunnen worden uitgesloten - is hiervan nog geen sprake. Voorts moet de verstrekking van de gegevens niet verder gaan dan nodig is voor het doel waarvoor deze worden gevraagd. Bij het collectief afsluiten van een verzekering kan met het verstrekken van totaalcijfers over ziekteverzuim en instroom in de WAO worden volstaan.

Hoe groter de inbreuk op de persoonlijke levenssfeer van de werknemers is, hoe meer reden er is om toestemming voor de verstrekking te vragen of extra waarborgen te treffen. Goede informatie aan betrokkenen of de mogelijkheid om vooraf bezwaar te maken tegen de gegevensverstrekking bieden daarvoor mogelijkheden. Aan de vraag of in concreto de ANW-hiaatverzekering was te beschouwen als een voor personeelsleden geldende arbeidsvoorwaarde kwam de Registratiekamer niet toe, nu de directie heeft nagelaten uitdrukkelijk te beoordelen of de gegevensverstrekking 'noodzakelijk' was. Evenmin is de betrokken werknemers om toestemming gevraagd. De conclusie moet dan ook zijn, dat de werkgever niet gerechtigd was om op de wijze waarop dit heeft plaatsgevonden, gegevens over ziekteverzuim en WAO van individuele werknemers te verstrekken aan een verzekeringsmaatschappij.

Persberichten dat een verzekeringsmaatschappij Arbo-diensten verplicht om bepaalde verzuimgegevens van werknemers te registreren en aan de verzekeringsmaatschappij te verstrekken waren eveneens aanleiding voor de Registratiekamer om een onderzoek in te stellen. Nieuw was, zo bleek uit het onderzoek, dat een verzekeringsmaatschappij in het kader van de verzuimverzekering de werkgever verplichtte om de Arbo-dienst bepaalde persoonsgegevens te laten registreren. De vraag is of de registratie van de gespecificeerde gegevens past binnen het doel van de registratie van een Arbo-dienst. De Registratiekamer is van oordeel dat registratie van de met name genoemde gegevens, gelet op de wettelijke verplichting voor de werkgever om een ziekteverzuimbeleid te voeren en daarbij een Arbo-dienst in te schakelen, het redelijk belang van de Arbo-dienst niet te buiten gaat.

De verplichting tot verstrekking van verzuimgegevens aan de verzekeringsmaatschappij is geconcretiseerd in een 'Verzuimstaat'. De Registratiekamer toetst deze aan het Protocol gegevensuitwisseling tussen Arbo-diensten en verzekeraars op het gebied van verzuim van werknemers. Het protocol is op 5 maart 1999 goedgekeurd door de Registratiekamer. De onderzochte verstrekking blijft grotendeels binnen het kader van het Protocol en is dus toegestaan.

Marketing met werknemersgegevens

Organen die met de uitvoering van sociale verzekeringen belast zijn, verrichten vaak ook (commerciële) nevenactiviteiten. De vraag doet zich daarbij regelmatig voor of zij hiervoor gebruik mogen maken van de hen in het kader van de uitvoering van de publieke taak ter beschikking gestelde werknemersgegevens. Zo hebben bouwbedrijven bij de Registratiekamer aangegeven dat werknemers bij hun vakantierechtenoverzicht ook een folder van een uitzendbureau ontvangen. De werknemers zijn op grond van de geldende CAO's verplicht om hun vakantierechten door het Vakantiefonds te administreren. Het Vakantiefonds maakt deel uit van het SFB en had de administratie uitbesteed aan SFB Diensten, een dochtermaatschappij in de zogenaamde B-poot, het private deel van het SFB. Toen aan de werknemers het vakantierechtenoverzicht werd verstuurd, werd ook een folder meegezonden van een uitzendbureau in de bouw, een andere dochtermaatschappij in de B-poot.

Voor de Registratiekamer was de kernvraag of het verzorgen van de mailing in opdracht van het Vakantiefonds, voor uitzendbureau X verenigbaar is met het doel van de persoonsregistratie, waaruit de NAW-gegevens afkomstig zijn. Het verplichte karakter van de vakantierechten-registratie stelt volgens de Registratiekamer striktere grenzen aan het verenigbaar gebruik. De mailing is naar alle deelnemers gezonden. Om de mailing te verzenden is gebruik gemaakt van de NAW-gegevens van de werknemers. Het gebruik is dus beperkt gebleven tot gegevens die in het algemeen niet bijzonder privacygevoelig zijn. Verder heeft de Registratiekamer in aanmerking genomen dat het attenderen van de deelnemers op werkgelegenheid in de bouw in het verlengde ligt van de relatie tussen het Vakantiefonds en werknemers. In de bouwsector worden veel tijdelijke contracten gesloten en wisselen veel werknemers regelmatig van werkgever. Onder deze omstandigheden kan het meesturen van de folder door een fonds dat een deel van de collectieve arbeidsvoorwaarden uitvoert als 'verwant' worden beschouwd. De betrokken werknemers kunnen er tenslotte ook zelf belang bij hebben op de hoogte te worden gehouden van de werkgelegenheid in de bouw en de mogelijkheid om via de bemiddeling van een uitzendbureau weer aan de slag te komen. Het ontvangen van de mailing valt niet buiten hetgeen werknemers in de bouw redelijkerwijs van het Vakantiefonds mogen verwachten. Dit leidt tot de conclusie van de Registratiekamer dat het (laten)verzorgen van de mailing voor het uitzendbureau, verenigbaar is met het doel van de registratie van het Vakantiefonds en geoorloofd was.

Het gebruik van medische gegevens door een zorgverzekeraar

Een verzekeraar heeft uit haar verzekerdenbestand een selectie gemaakt voor het verspreiden van de diabetespas. Aan de Registratiekamer is gevraagd of de wijze waarop de verzekeraar de diabetespas heeft verspreid, verenigbaar is met het doel van zijn verzekerdenbestand. Het doel van de verspreiding van de diabetespas is verzekerden die aan de chronische ziekte diabetes mellitus lijden, bewust te maken van hun eigen inbreng in hun gezondheidstoestand. De selectie van diabetespatiënten vond plaats aan de hand van declaraties voor bepaalde geneesmiddelen.

De verzekeraar heeft deze diabetes mellitus als eerste ziektebeeld gekozen in het kader van het ontwikkelen van disease management programma's. Deze zijn gericht op een integrale benadering van preventie, diagnostiek en behandeling van een bepaalde chronische ziekte. Het leveren van een bijdrage aan de kwaliteit van het leven van de patiënten en het beperken van de schadelast van de verzekeraar zijn doeleinden van deze programma's.

De Registratiekamer heeft beoordeeld of het gebruik van de declaratiegegevens door de verzekeraar als 'verenigbaar gebruik' kan worden beschouwd. De Registratiekamer heeft geconcludeerd dat bij het beoogde geheel wel sprake is van een zekere verwantschap met het primaire doel van de rechtsverhouding tussen verzekeraar en verzekerde, maar dat er ook sprake is van omstandigheden die bijzondere aandacht vergen. De aard van de gebruikte gegevens en de wijze waarop deze zijn verkregen brengt met zich mee dat striktere eisen dienen te worden gesteld aan de doelbinding. Het gaat namelijk om een specifieke groep patiënten met een bepaald ziektebeeld. Deze laatste omstandigheid leidt ertoe dat tevens rekening dient te worden gehouden met de striktere beperkingen die zijn gesteld over de verwerking van medische gegevens. Voor het verwerken van medische gegevens gelden strikte beperkingen. De Registratiekamer acht het gebruik van medische gegevens voor de verspreiding van de diabetespas niet noodzakelijk voor de uitvoering van een verzekeringsovereenkomst, dan wel voor de goede uitvoering van de Ziekenfondswet (ZFW) of de Algemene Wet Bijzondere Ziektekosten (AWBZ).

Van negatieve gevolgen voor de verzekerden is niets gebleken. De Registratiekamer onderkent de serviceaspecten van de Diabetespas. De belangenorganisaties van diabetespatiënten zijn bij de realisering van het project betrokken, evenals de zorgverleners die bij deze belangenorganisaties zijn aangesloten. De verzekerden zijn echter van tevoren niet geïnformeerd over de voorgenomen aanbidding van de pas en hen is ook niet de mogelijkheid geboden bezwaar te maken tegen de voorgenomen werkwijze of daarmee in te stemmen.

De Registratiekamer komt tot de conclusie dat de verzekeraar bij de verspreiding van de diabetespas buiten de verzekeringsovereenkomst, de ZFW of de AWBZ is getreden. De gegevens van verzekerden zijn gebruikt voor een doel dat - zonder nadere waarborgen - niet verenigbaar was met het doel waarvoor die gegevens verkregen zijn. Omdat een specifieke groep verzekerden met een bepaald ziektebeeld is geselecteerd, had alleen de uitdrukkelijke (schriftelijke) toestemming van de betrokken verzekerden dit gebrek kunnen repareren. De Registratiekamer heeft tevens opgemerkt dat de gevolgde handelwijze dreigt te treden in de rechtsverhouding tussen patiënt en zorgverlener. Er was geen legitieme grond voor bemoeienis van de verzekeraar met de individuele zorgverlening. Het verstrekken van de diabetespas is een eerste stap in de Disease Management-programma's. De Registratiekamer heeft het belang van het treffen van adequate privacywaarborgen daarbij benadrukt om ongewenste grensoverschrijdingen te voorkomen. Ten slotte signaleert de Registratiekamer een risicovolle ontwikkeling bij vermenging van het belang van de verzekeraar bij kostenbeheersing en de taak toe te zien op de inhoudelijke kwaliteit van de zorg door de zorgverlener. Onderdeel van de gewenste waarborgen is het samenwerken met beroeps- en patiëntenorganisaties, maar de eigen rol van de betrokkenen patiënten of verzekerden mag daarbij niet uit het oog worden verloren.

Technology Assessment

Het jaar 1999 stond in het teken van de overgang van de uit 1989 daterende Wet persoonsregistraties naar de Wet Bescherming Persoonsgegevens. De sterk veranderde aard en inzet van informatie en communicatietechnologie in de afgelopen tien jaar wordt weerspiegeld in deze wet. Waar in de jaren tachtig computers vaak losstaande machines waren, zien we aan het eind van de jaren negentig grootschalige koppelingen van computers, met als meest vergaande vorm de wereldwijde koppeling van computernetwerken aan het internet. In deze situatie is het niet langer zinvol om het wettelijke kader te beperken tot de vastlegging van gegevens in persoonsregistraties. De nieuwe wetgeving heeft dan ook betrekking op de ruimer geformuleerde verwerking van persoonsgegevens. Hieronder worden alle mogelijke processen verstaan die met persoonsgegevens worden verricht, van het moment van het genereren of vergaren van de gegevens tot en met het moment waarop de gegevens vernietigd worden.

Het aantal processen waarin persoonsgegevens verwerkt wordt, is door de technologische ontwikkelingen sterk gegroeid. Binnen het kader van haar wettelijke taken voert de Registratiekamer een programma van *technology assessments* uit, waarin wordt nagegaan welke technologieën dreigingen inhouden voor de privacy en in hoeverre technologie juist ingezet kan worden als middel voor de bescherming van privacy. De uitkomsten van deze studies zijn bepalend voor het standpunt van de Registratiekamer ten opzichte van deze technologieën.

Privacy Enhancing Technologies

Een belangrijke denkrichting is de inzet van technologie voor het verminderen van de hoeveelheid persoonsgegevens die binnen informatiesystemen worden verwerkt. In conventionele informatiesystemen worden veelal onnodig grote hoeveelheden informatie over personen vastgelegd. Door de groeiende mogelijkheden van computers en netwerken worden steeds meer koppelingen aangebracht met andere persoonsgegevens, waardoor het gehalte aan informatie over personen binnen de systemen onnodig groeit. Om dit te voorkomen dienen informatiesystemen te worden aangepast. Het rapport *Privacy Enhancing Technologies; the path to anonymity* geeft opties om met behulp van informatietechnologie het aantal persoonsgegevens binnen een systeem te beperken, dan wel de opname van nieuwe – niet essentiële – persoonsgegevens te voorkomen. Overigens kan bij gebruik van deze *Privacy Enhancing Technologies (PET)* dikwijls de gewenste functionaliteit van het systeem onaangetast blijven.

Een optie is bij het gebruik geen identificerende gegevens te genereren of vast te leggen. De afwezigheid van identificerende data en datasporen maakt het dan onmogelijk om aanwezige gegevens in verband te brengen met een individu. Een andere mogelijkheid is het opnemen van een extra element in het conventionele informatiesysteem, de Identiteitsbeschermer, waardoor het mogelijk is om de privacy van de gebruikers van het systeem te beschermen. Bij gebruikmaking van het systeem wordt dan telkens de gebruikersidentiteit omgezet in een, voor elke transactie unieke, pseudo-identiteit. De privacy van de geregistreerde wordt zo afdoende beschermd. Hierbij kan gebruik gemaakt worden van bestaande technieken zoals versleuteling, digitale handtekeningen en Trusted Third Parties.

De belangstelling voor het PET-concept is groeiende, mede omdat bij ontwikkelaars van software het besef doordringt dat de zorg voor een adequate privacybescherming tevens bijdraagt aan de verbetering van een informatiesysteem. Maatregelen om de privacy te

beschermen gaan bijvoorbeeld hand in hand met een goede beveiliging van systemen tegen onbevoegd gebruik. Het vertrouwen van gebruikers in een systeem neemt hierdoor veelal toe, waardoor ook de acceptatie en de mate van gebruik positief beïnvloed worden. Het initiatief tot het implementeren van PET wordt steeds vaker door en binnen diverse branches zelf genomen. De Registratiekamer heeft in de loop van 1999 wederom een groeiend aantal adviesvragen gehad van ontwikkelaars. Een leidende leverancier van grote datawarehouses uit de Verenigde Staten heeft in 1999 de PET-principes gebruikt voor de bouw van een datawarehouse met ingebouwde privacybescherming. Ook in de zorgsector is in het afgelopen jaar het PET-concept opgenomen in nieuwe informatiesystemen, bijvoorbeeld in de systemen met betrekking tot de verslavingszorg

Een bijzondere ontwikkeling in 1999 was de opname van de principes van PET, zoals door medewerking van de Registratiekamer ingebracht, in de wereldwijde ISO-norm waarmee informatiebeveiliging kan worden geëvalueerd, ISO/IEC 15408. Verder nam de Tweede Kamer tijdens de behandeling van de nieuwe privacywet kamerbreed een motie aan waarin de regering verzocht werd de ontwikkeling en het gebruik van PET krachtig ter hand te nemen en te bevorderen dat de overheid het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens.

Datamining en data warehousing

De marktbenadering van veel bedrijven, maar ook van de overheid, transformeert van massamarketing naar een steeds meer op het individu toegesneden aanbod van producten en diensten. Een doelgerichte benadering van groepen personen of individuen vereist een nauwgezet beeld van levensstijl, gewoonten, wensen en voorkeuren. Het samenstellen van profielen van consumenten is een voorwaarde voor een dergelijke segmentering van de markt. Informatietechnologie biedt daartoe nieuwe krachtige instrumenten: geordende opslag van zeer grote hoeveelheden persoonsgegevens in *data warehouses* is in volle gang. Met *data mining technieken* kan worden gezocht naar, niet van tevoren veronderstelde, samenhangen. De Registratiekamer heeft datamining en data warehousing onderkend als belangwekkend en daarom werd binnen het technology assessment programma een studie afgerond naar de privacyaspecten van deze technieken. In mei 1999 organiseerde de Registratiekamer een expertsessie waarin over de privacyaspecten van datamining werd gediscussieerd, waarvan verslag werd gedaan in *Privacy & Informatie*, nummer 3, juni 1999.

Software agents

Samen met TNO/FEL is in het afgelopen jaar een studie afgerond over Intelligent Software Agents.

Een 'agent' is een software programma dat min of meer zelfstandig taken kan uitvoeren voor zijn opdrachtgever. Agents, die ook wel elektronische slaven worden genoemd, zijn een product uit het vakgebied van de kunstmatige intelligentie. De belangstelling voor deze agents komt vooral voort uit het feit dat het voor mensen steeds moeilijker wordt om zonder tussenkomst wegwijs te worden in de grote hoeveelheden informatie die zich op grote computernetwerken bevinden. Zoekmachines op het internet worden gezien als een eerste generatie agents.

Er zijn echter meer geavanceerde agents in ontwikkeling die niet alleen informatie vergaren, maar ook op basis daarvan voor hun eigenaar zelfstandig transacties uitvoeren. De agents vertegenwoordigen daarbij hun eigenaar. Hiertoe wordt een agent voorzien van een profiel op basis van de persoonsgegevens van zijn eigenaar. Dit profiel bevat gegevens over voorkeuren, gebruiken, adresgegevens enzovoorts. Anderzijds kan een agent ook dergelijke informatie over anderen vergaren.

In de serie Achtergronden en Verkenningen is in samenwerking met de Canadese tegenhanger van de Registratiekamer, de Information and Privacy Officer in Ontario het rapport *'Intelligent software agents'* uitgebracht. In het rapport worden de thans in ontwikkeling zijnde agents geïnventariseerd, alsmede de privacy aspecten die te voorschijn komen wanneer deze autonoom te werk gaan als vertegenwoordiger van een natuurlijke persoon. Daarbij wordt aangegeven welke juridische grondbeginselen ten grondslag liggen aan de beoordeling van een agent. Overigens is de greep van het huidige wetgevende kader op dit fenomeen nog niet duidelijk, zo wordt geconstateerd. Tot slot bevat het rapport een aantal modellen aan de hand waarvan het PET-principe kan worden meegenomen bij de bouw van agents. Een internationaal consortium, waarvoor de Registratiekamer het initiatief nam, is in 1999 begonnen met een drie jaar durend project waarin aan de hand van deze modellen een werkzame software agent met ingebouwde privacy bescherming wordt gebouwd.

Internet en het gebruik van persoonsgegevens

Het sterk groeiend gebruik van internet zal zonder twijfel de meeste vragen rond privacy oproepen in de komende jaren. In 1999 heeft de EU-werkgroep van nationale toezichthouders op het terrein van de privacybescherming, als bedoeld in artikel 29 van de Europese privacyrichtlijn, een expertgroep in het leven geroepen die zich specifiek richt op de uitleg van de relevante Europese richtlijnen voor het internetgebruik.

Gedurende het jaar heeft de Internet Task Force, waaraan ook de Registratiekamer deelneemt, een aantal standpunten voor de werkgroep voorbereid. Eén van de uitgebrachte standpunten betreft een oproep aan ontwikkelaars van software en hardware om te voorkomen dat ongemerkt persoonsgegevens verzameld worden bij internetgebruik. Voorbeelden van dergelijk 'onzichtbare gegevensverwerkingen' zijn cookies, kleine tekstbestanden die veelal ongemerkt worden meegezonden wanneer iemand een website bezoekt. Deze cookies worden op de harde schijf van de gebruiker geplaatst en kunnen gebruikt worden voor het verzamelen van gegevens over het bezoek aan websites. Ook heeft de aanbeveling betrekking op serienummers van software of hardware die ongemerkt worden meegezonden bij het internetgebruik en die kunnen dienen ter identificatie van de gebruikte computer. De werkgroep beveelt ontwikkelaars aan gebruikers volledig op de hoogte te stellen van het inwinnen van iemands gegevens. Verder moeten gebruikers de mogelijkheid hebben het inwinnen van gegevens te voorkomen.

Een andere standpunt van de werkgroep, voorbereid voor de Internet Task Force, betrof de tijdsduur gedurende welke Internet Service Providers wettelijk gehouden zijn aan het bewaren van iemands gegevens over internetgebruik voor wettelijke handhavingstaken. Er werd gepleit voor een limiet van niet langer dan drie maanden.

Het werkprogramma voor het jaar 2000 voorziet in een uiteenzetting over de werking van de Europese richtlijnen over de bescherming van persoonsgegevens op veel uitgevoerde handelingen op het internet, zoals e-mailen, surfen en zoeken.

Biometrische identificatie

In 1999 werd de doorbraak van systemen voor biometrische identificatie en authenticatie zichtbaar. Deze systemen worden gebruikt voor identificatie, het vaststellen van iemands identiteit, of voor authenticatie, het bevestigen van een door iemand geclaimde identiteit. Daartoe wordt een lichaamskenmerk geregistreerd en opgeslagen in een database. Wanneer iemand zich moet identificeren, bijvoorbeeld bij de toegang tot een gebouw of bij het

gebruikmaken van een geldautomaat, presenteert hij het bewuste lichaamskenmerk, bijvoorbeeld zijn vingerafdruk, dat vervolgens wordt vergeleken met het in de database vastgelegde kenmerk. Het grote voordeel hiervan is dat lichaamskenmerken uniek zijn, en nagenoeg niet te vervalsen of over te dragen aan een andere persoon. Dit laatste in tegenstelling tot gangbare methoden als pincodes die kunnen worden overgedragen, met de daarbij behorende risico voor fraude of andere vormen van onbevoegd gebruik.

Vanuit privacyoogpunt plaatst de Registratiekamer kanttekeningen bij grootschalige invoering van biometrische systemen. Het unieke karakter van lichaamskenmerken, houdt tevens een risico in. Wanneer zij namelijk in databases worden opgeslagen bieden biometrische gegevens een sleutel die uniek aan een persoon gebonden is, met de mogelijkheid om bij koppeling van bestanden de handelingen van een persoon volledig te traceren. Door de inzet van biometrische identificatie die ongemerkt geschiedt, bijvoorbeeld door middel van automatische gezichtsherkennig of stemherkenning over telecommunicatie verbindingen, staat tevens de mogelijkheid van anoniem deel te nemen aan het maatschappelijk verkeer onder druk. Bovendien kan het biometrische gegeven zelf ook informatie bevatten die ver voorbij gaat aan het eigenlijke doel van vastlegging, bijvoorbeeld over het ras, de gezondheidstoestand of de emotionele toestand.

Met het oog op deze vraagstukken heeft de Registratiekamer samen met TNO/FEL een studie verricht waarin de privacy aspecten van biometrie, het relevante juridische kader en de mogelijke PET-oplossingen worden uiteengezet. Daarbij is uitgegaan van de Europese privacy richtlijn 95/46/EG die grotendeels overeenkomt met de, naar verwachting in 2000 in werking tredende, Wet Bescherming Persoonsgegevens. Het rapport '*At face value, on biometrical identification and privacy*' werd op 5 oktober aangeboden aan de minister van Grote Stedenbeleid. De minister heeft bij die gelegenheid en in de Tweede Kamer toegezegd de bevindingen uit het rapport te betrekken bij de ontwikkeling van een nieuwe generatie reisdocumenten met biometrisch kenmerk. Organisaties uit binnen- en buitenland toonden hun belangstelling voor het rapport dat al binnen een maand aan een herdruk toe was.

Technology Assessment

Het jaar 1999 stond in het teken van de overgang van de uit 1989 daterende Wet persoonsregistraties naar de Wet Bescherming Persoonsgegevens. De sterk veranderde aard en inzet van informatie en communicatietechnologie in de afgelopen tien jaar wordt weerspiegeld in deze wet. Waar in de jaren tachtig computers vaak losstaande machines waren, zien we aan het eind van de jaren negentig grootschalige koppelingen van computers, met als meest vergaande vorm de wereldwijde koppeling van computernetwerken aan het internet. In deze situatie is het niet langer zinvol om het wettelijke kader te beperken tot de vastlegging van gegevens in persoonsregistraties. De nieuwe wetgeving heeft dan ook betrekking op de ruimer geformuleerde verwerking van persoonsgegevens. Hieronder worden alle mogelijke processen verstaan die met persoonsgegevens worden verricht, van het moment van het genereren of vergaren van de gegevens tot en met het moment waarop de gegevens vernietigd worden.

Het aantal processen waarin persoonsgegevens verwerkt wordt, is door de technologische ontwikkelingen sterk gegroeid. Binnen het kader van haar wettelijke taken voert de Registratiekamer een programma van *technology assessments* uit, waarin wordt nagegaan welke technologieën dreigingen inhouden voor de privacy en in hoeverre technologie juist ingezet kan worden als middel voor de bescherming van privacy. De uitkomsten van deze studies zijn bepalend voor het standpunt van de Registratiekamer ten opzichte van deze technologieën.

Privacy Enhancing Technologies

Een belangrijke denkrichting is de inzet van technologie voor het verminderen van de hoeveelheid persoonsgegevens die binnen informatiesystemen worden verwerkt. In conventionele informatiesystemen worden veelal onnodig grote hoeveelheden informatie over personen vastgelegd. Door de groeiende mogelijkheden van computers en netwerken worden steeds meer koppelingen aangebracht met andere persoonsgegevens, waardoor het gehalte aan informatie over personen binnen de systemen onnodig groeit. Om dit te voorkomen dienen informatiesystemen te worden aangepast. Het rapport *Privacy Enhancing Technologies; the path to anonymity* geeft opties om met behulp van informatietechnologie het aantal persoonsgegevens binnen een systeem te beperken, dan wel de opname van nieuwe – niet essentiële – persoonsgegevens te voorkomen. Overigens kan bij gebruik van deze *Privacy Enhancing Technologies (PET)* dikwijls de gewenste functionaliteit van het systeem onaangetast blijven.

Een optie is bij het gebruik geen identificerende gegevens te genereren of vast te leggen. De afwezigheid van identificerende data en datasporen maakt het dan onmogelijk om aanwezige gegevens in verband te brengen met een individu. Een andere mogelijkheid is het opnemen van een extra element in het conventionele informatiesysteem, de Identiteitsbeschermer, waardoor het mogelijk is om de privacy van de gebruikers van het systeem te beschermen. Bij gebruikmaking van het systeem wordt dan telkens de gebruikersidentiteit omgezet in een, voor elke transactie unieke, pseudo-identiteit. De privacy van de geregistreerde wordt zo afdoende beschermd. Hierbij kan gebruik gemaakt worden van bestaande technieken zoals versleuteling, digitale handtekeningen en Trusted Third Parties.

De belangstelling voor het PET-concept is groeiende, mede omdat bij ontwikkelaars van software het besef doordringt dat de zorg voor een adequate privacybescherming tevens bijdraagt aan de verbetering van een informatiesysteem. Maatregelen om de privacy te

beschermen gaan bijvoorbeeld hand in hand met een goede beveiliging van systemen tegen onbevoegd gebruik. Het vertrouwen van gebruikers in een systeem neemt hierdoor veelal toe, waardoor ook de acceptatie en de mate van gebruik positief beïnvloed worden. Het initiatief tot het implementeren van PET wordt steeds vaker door en binnen diverse branches zelf genomen. De Registratiekamer heeft in de loop van 1999 wederom een groeiend aantal adviesvragen gehad van ontwikkelaars. Een leidende leverancier van grote datawarehouses uit de Verenigde Staten heeft in 1999 de PET-principes gebruikt voor de bouw van een datawarehouse met ingebouwde privacybescherming. Ook in de zorgsector is in het afgelopen jaar het PET-concept opgenomen in nieuwe informatiesystemen, bijvoorbeeld in de systemen met betrekking tot de verslavingszorg

Een bijzondere ontwikkeling in 1999 was de opname van de principes van PET, zoals door medewerking van de Registratiekamer ingebracht, in de wereldwijde ISO-norm waarmee informatiebeveiliging kan worden geëvalueerd, ISO/IEC 15408. Verder nam de Tweede Kamer tijdens de behandeling van de nieuwe privacywet kamerbreed een motie aan waarin de regering verzocht werd de ontwikkeling en het gebruik van PET krachtig ter hand te nemen en te bevorderen dat de overheid het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens.

Datamining en data warehousing

De marktbenadering van veel bedrijven, maar ook van de overheid, transformeert van massamarketing naar een steeds meer op het individu toegesneden aanbod van producten en diensten. Een doelgerichte benadering van groepen personen of individuen vereist een nauwgezet beeld van levensstijl, gewoonten, wensen en voorkeuren. Het samenstellen van profielen van consumenten is een voorwaarde voor een dergelijke segmentering van de markt. Informatietechnologie biedt daartoe nieuwe krachtige instrumenten: geordende opslag van zeer grote hoeveelheden persoonsgegevens in *data warehouses* is in volle gang. Met *data mining technieken* kan worden gezocht naar, niet van tevoren veronderstelde, samenhangen. De Registratiekamer heeft datamining en data warehousing onderkend als belangwekkend en daarom werd binnen het technology assessment programma een studie afgerond naar de privacyaspecten van deze technieken. In mei 1999 organiseerde de Registratiekamer een expertsessie waarin over de privacyaspecten van datamining werd gediscussieerd, waarvan verslag werd gedaan in *Privacy & Informatie*, nummer 3, juni 1999.

Software agents

Samen met TNO/FEL is in het afgelopen jaar een studie afgerond over Intelligent Software Agents.

Een 'agent' is een software programma dat min of meer zelfstandig taken kan uitvoeren voor zijn opdrachtgever. Agents, die ook wel elektronische slaven worden genoemd, zijn een product uit het vakgebied van de kunstmatige intelligentie. De belangstelling voor deze agents komt vooral voort uit het feit dat het voor mensen steeds moeilijker wordt om zonder tussenkomst wegwijs te worden in de grote hoeveelheden informatie die zich op grote computernetwerken bevinden. Zoekmachines op het internet worden gezien als een eerste generatie agents.

Er zijn echter meer geavanceerde agents in ontwikkeling die niet alleen informatie vergaren, maar ook op basis daarvan voor hun eigenaar zelfstandig transacties uitvoeren. De agents vertegenwoordigen daarbij hun eigenaar. Hiertoe wordt een agent voorzien van een profiel op basis van de persoonsgegevens van zijn eigenaar. Dit profiel bevat gegevens over voorkeuren, gebruiken, adresgegevens enzovoorts. Anderzijds kan een agent ook dergelijke informatie over anderen vergaren.

In de serie Achtergronden en Verkenningen is in samenwerking met de Canadese tegenhanger van de Registratiekamer, de Information and Privacy Officer in Ontario het rapport *'Intelligent software agents'* uitgebracht. In het rapport worden de thans in ontwikkeling zijnde agents geïnterpreteerd, alsmede de privacy aspecten die te voorschijn komen wanneer deze autonoom te werk gaan als vertegenwoordiger van een natuurlijke persoon. Daarbij wordt aangegeven welke juridische grondbeginselen ten grondslag liggen aan de beoordeling van een agent. Overigens is de greep van het huidige wetgevende kader op dit fenomeen nog niet duidelijk, zo wordt geconstateerd. Tot slot bevat het rapport een aantal modellen aan de hand waarvan het PET-principe kan worden meegenomen bij de bouw van agents. Een internationaal consortium, waarvoor de Registratiekamer het initiatief nam, is in 1999 begonnen met een drie jaar durend project waarin aan de hand van deze modellen een werkzame software agent met ingebouwde privacy bescherming wordt gebouwd.

Internet en het gebruik van persoonsgegevens

Het sterk groeiend gebruik van internet zal zonder twijfel de meeste vragen rond privacy oproepen in de komende jaren. In 1999 heeft de EU-werkgroep van nationale toezichthouders op het terrein van de privacybescherming, als bedoeld in artikel 29 van de Europese privacyrichtlijn, een expertgroep in het leven geroepen die zich specifiek richt op de uitleg van de relevante Europese richtlijnen voor het internetgebruik.

Gedurende het jaar heeft de Internet Task Force, waaraan ook de Registratiekamer deelneemt, een aantal standpunten voor de werkgroep voorbereid. Eén van de uitgebrachte standpunten betreft een oproep aan ontwikkelaars van software en hardware om te voorkomen dat ongemerkt persoonsgegevens verzameld worden bij internetgebruik. Voorbeelden van dergelijk 'onzichtbare gegevensverwerkingen' zijn cookies, kleine tekstbestanden die veelal ongemerkt worden meegezonden wanneer iemand een website bezoekt. Deze cookies worden op de harde schijf van de gebruiker geplaatst en kunnen gebruikt worden voor het verzamelen van gegevens over het bezoek aan websites. Ook heeft de aanbeveling betrekking op serienummers van software of hardware die ongemerkt worden meegezonden bij het internetgebruik en die kunnen dienen ter identificatie van de gebruikte computer. De werkgroep beveelt ontwikkelaars aan gebruikers volledig op de hoogte te stellen van het inwinnen van iemands gegevens. Verder moeten gebruikers de mogelijkheid hebben het inwinnen van gegevens te voorkomen.

Een andere standpunt van de werkgroep, voorbereid voor de Internet Task Force, betrof de tijdsduur gedurende welke Internet Service Providers wettelijk gehouden zijn aan het bewaren van iemands gegevens over internetgebruik voor wettelijke handhavingstaken. Er werd gepleit voor een limiet van niet langer dan drie maanden.

Het werkprogramma voor het jaar 2000 voorziet in een uiteenzetting over de werking van de Europese richtlijnen over de bescherming van persoonsgegevens op veel uitgevoerde handelingen op het internet, zoals e-mailen, surfen en zoeken.

Biometrische identificatie

In 1999 werd de doorbraak van systemen voor biometrische identificatie en authenticatie zichtbaar. Deze systemen worden gebruikt voor identificatie, het vaststellen van iemands identiteit, of voor authenticatie, het bevestigen van een door iemand geclaimde identiteit. Daartoe wordt een lichaamskenmerk geregistreerd en opgeslagen in een database. Wanneer iemand zich moet identificeren, bijvoorbeeld bij de toegang tot een gebouw of bij het gebruikmaken van een geldautomaat, presenteert hij het bewuste lichaamskenmerk, bijvoorbeeld zijn vingerafdruk, dat vervolgens wordt vergeleken met het in de database vastgelegde kenmerk. Het grote voordeel hiervan is dat lichaamskenmerken uniek zijn, en nagenoeg niet te vervalsen of over te dragen aan een andere persoon. Dit laatste in tegenstelling tot gangbare methoden als pincodes die kunnen worden overgedragen, met de daarbij behorende risico voor fraude of andere vormen van onbevoegd gebruik.

Vanuit privacyoogpunt plaatst de Registratiekamer kanttekeningen bij grootschalige invoering van biometrische systemen. Het unieke karakter van lichaamskenmerken, houdt tevens een risico in. Wanneer zij namelijk in databases worden opgeslagen bieden biometrische gegevens een sleutel die uniek aan een persoon gebonden is, met de mogelijkheid om bij koppeling van bestanden de handelingen van een persoon volledig te traceren. Door de inzet van biometrische identificatie die ongemerkt geschiedt, bijvoorbeeld door middel van automatische gezichtsherkennig of stemherkenning over telecommunicatie verbindingen, staat

tevens de mogelijkheid van anoniem deel te nemen aan het maatschappelijk verkeer onder druk. Bovendien kan het biometrische gegeven zelf ook informatie bevatten die ver voorbij gaat aan het eigenlijke doel van vastlegging, bijvoorbeeld over het ras, de gezondheidstoestand of de emotionele toestand.

Met het oog op deze vraagstukken heeft de Registratiekamer samen met TNO/FEL een studie verricht waarin de privacy aspecten van biometrie, het relevante juridische kader en de mogelijke PET-oplossingen worden uiteengezet. Daarbij is uitgegaan van de Europese privacy richtlijn 95/46/EG die grotendeels overeenkomt met de, naar verwachting in 2000 in werking tredende, Wet Bescherming Persoonsgegevens. Het rapport '*At face value, on biometrical identification and privacy*' werd op 5 oktober aangeboden aan de minister van Grote Stedenbeleid. De minister heeft bij die gelegenheid en in de Tweede Kamer toegezegd de bevindingen uit het rapport te betrekken bij de ontwikkeling van een nieuwe generatie reisdocumenten met biometrisch kenmerk. Organisaties uit binnen- en buitenland toonden hun belangstelling voor het rapport dat al binnen een maand aan een herdruk toe was.

Organisatie

In het verslagjaar heeft de Registratiekamer veel aandacht geschonken aan de eigen organisatie en de interne werkwijze. Natuurlijk is daarvoor goed geluisterd naar feedback op het eigen functioneren in het verleden. De eigen behoefte om de bedrijfsvoering en effectiviteit te verbeteren is gecombineerd met de veranderingen die nodig zijn met de komst van de nieuwe Wet bescherming persoonsgegevens.

In de loop van het jaar is bij steeds meer gelegenheden helderheid gegeven over de positionering van de Registratiekamer. Nuchterheid is een sleutelwoord waarmee de Registratiekamer haar optreden wil typeren: met oog voor de praktijk toezicht houden op de behoorlijke uitvoering van de wetgeving op de verwerking van persoonsgegevens. Die taak krijgt inmiddels vorm door een scala van activiteiten, waarbij de Registratiekamer steeds meer pro-actief optreedt. Door het publiceren van vernieuwend onderzoek wordt bijgedragen aan een behoorlijke verwerking van persoonsgegevens. Het onderzoeken en uitdragen van nieuwe mogelijkheden om de technologie ten gunste van een behoorlijke verwerking van persoonsgegevens in te zetten (Privacy Enhancing Technology= PET) is een ander belangrijk voorbeeld van pro-actief optreden. De Registratiekamer wil haar aandacht en capaciteit meer besteden aan dit soort activiteiten. Zij wil in die zin steeds meer gaan functioneren als een tweedelijns-organisatie. Het stimuleren en ondersteunen van branches en sectoren tot zelfregulering en gedragscodes is daarvan een voorbeeld.

De interne organisatie en werkwijze is afgestemd op deze taakopvatting. Door werkprocessen te stroomlijnen en te standaardiseren is capaciteit vrijgemaakt om initiatieven in het kader van de doelstellingen te realiseren. De eerstelijns-activiteiten (zoals het beantwoorden van publieksvragen) blijven adequaat uitgevoerd. Door introductie van de nog groeiende internetsite (www.registratiekamer.nl) wordt een aantal publieksvragen al direct beantwoord, zonder directe tussenkomst van medewerkers van de Registratiekamer. Voor de eerste opvang van overige telefonische en schriftelijke publieksvragen is in de interne organisatie een frontoffice afgesplitst. Daar worden verzoeken en klachten op grond van vooraf vastgestelde criteria op een adequate, snelle en consistente manier behandeld. In 1999 werd 21% van alle verzoeken door het frontoffice behandeld. Voor het frontoffice geldt een aangepaste (standaard) werkwijze met maximaal gebruik van voorlichtingsmateriaal. Door een duidelijke splitsing van de werkwijze in twee organisatorische eenheden, te weten het frontoffice en het backoffice, wordt een snellere publieksservice gerealiseerd met een beperkter capaciteitsbeslag waardoor ruimte is gevonden voor activiteiten als tweedelijns-organisatie.

Sommige publieksvragen vergen meer studie en overweging, waarbij ook teruggegrepen kan worden op eerdere standpunten van de Registratiekamer. Daarvoor blijft maatwerk door het backoffice het passende antwoord. Gevoelige correspondentie, waarbij de Registratiekamer zich bijvoorbeeld voor het eerst uitspreekt over een beleidsvraag, inhoudelijke norm of wetgevingsadvies, vergt uiteraard nog meer interne aandacht en afstemming. Voor deze laatste categorieën correspondentie geldt dan ook de meest uitgebreide interne procedure.

De toegenomen initiatieven in samenwerking met branche- en koepelorganisaties worden meestal als project uitgevoerd. De methode van projectmanagement is aangescherpt om op tijd de gewenste resultaten te kunnen realiseren. Daarmee ontstaat niet alleen intern een betere afstemming en productiviteit. Ook in samenwerking met externe organisaties kan de Registratiekamer beter een bijdrage leveren.

De grotere variatie in taken en activiteiten, die op deze wijze wordt gerealiseerd, en de introductie van nieuwe werkwijzen en methoden heeft ook gevolgen voor het personeel. In overleg met de medewerkers zijn de gevolgen van de gewenste positionering voor werkwijze en inzet van de beschikbare capaciteit vastgesteld. In 1999 is bovendien de beschikbare vacatureruimte ingezet voor het vergroten van de differentiatie in achtergrond en ervaring van beleidsmedewerkers.

Tot slot is in 1999 extra aandacht besteed aan het verbeteren van de jaarplancyclus. Het werkprogramma van de Registratiekamer zal daardoor niet alleen winnen aan focus en samenhang, maar door concentratie op welgekozen projecten kan ook de impact en effectiviteit toenemen. Onderdeel van deze planvorming zal in ieder geval ook zijn een juiste maatvoering in onderwerpen en ambities: wie teveel tegelijk wil, loopt het risico te weinig te realiseren.

De gevolgen van de interne organisatorische, personele en procedurele maatregelen zullen vanaf het jaarprogramma 2000 merkbaar zijn.

Ondernemingsraad

Een groeiend aantal personeelsleden heeft ertoe geleid dat ook het aantal leden van de Ondernemingsraad (OR) is toegenomen. De OR bestaat sinds de verkiezingen van november 1999 uit vijf leden.

Bijlage 1 Aanmeldingen

Persoonsregistraties aangemeld bij de Registratiekamer van 1 januari 1999 tot en met 31 december 1999, gespecificeerd naar sector.

Landbouw en visserij	5
Delfstoffenwinning	0
Uitgeverijen	7
Geneesmiddelenfabrieken	2
Industrie overig	3
Sociale werkplaatsen	0
Nutsbedrijven	1
Bouwnijverheid	2
Auto- en garagebedrijven	17
Apothekers	3
Postorderbedrijven	3
Opticiëns	0
Handel overig	31
Goederenvervoer	1
Personenvervoer	4
Luchtvaartmaatschappijen	3
Verkeers- en toeristenbureau's	0
Post- telefoon- en telegraafdiensten	18
Transport/opslag/communicatiebedrijv.overig	2
Beleggingsmaatschappijen	5
Banken	5
Hypotheekbanken	2
Financieringsbemiddeling	201
Creditcardorganisaties	1
BKR	0
Bankwezen overig	1
Ziektekostenverzekeringen	3
Levensverzekeringen	2
Schadeverzekeringen	3
Pensioenfondsen	0
Assurantiebemiddeling	16
Verzekeringswezen overig	28
(Woning)bouwverenigingen/stg/coöperaties	5
Eigenaarsverenigingen	0
Makelaarskantoren	8
Exploitatie/handel onroerend goed overig	3
Rechtskundige diensten	1
Advokaten	9
Rechtskundige adviesbureau's	2
Notarissen	3
Deurwaarders	1
Accountantburo's	1
Boekhoudburo's en administratiekantoren	30
Belastingadviesburo's	1
Accountants-/boekhoudbureau's etc. overig	3

Computercentra en softwarebureau's	1
Reclame-, advertentiebureau's e.d.	0
Direct marketing	126
Telemarketing	21
Economisch adviesbureau's	4
Persbureau's, nieuwsbureau's	0
Uitzendbureau's	5
Arbeidsvoorziening	6
Arbeidsbemiddeling/Werving en Selectie	60
Uitzend-/uitleenbedrijven arbeidsbem.overig	47
Bureau's psychotechnische personeelsteden	0
Informatiebureau's	0
Incassobureau's	4
Recherche- c.q. detectivebureau's	36
Kredietinformatiebureaus (personen)	0
Handelsinformatiebureaus (bedrijven)	2
Bewaking- en beveiligingsdiensten	61
Zakelijke dienstverlening overig	10
Verhuur machines + andere roerende goederen	0
Overheid algemeen	0
Rijksoverheid	87
Provinciale overheid	2
Gemeentelijke overheid	70
Intergemeentelijke samenwerkingsverbanden	1
Waterschappen	0
Rechterlijke macht	1
Openbaar Ministerie	1
Gevangeniswezen	0
TBR/TBS kliniek	0
Kinderbescherming	0
Reclassering	0
Rechterlijke org.gevangenisw.,reclass. ov.	1
Politie	23
Bijzondere opsporingsdiensten	2
Ziekenfondsen	0
Bedrijfsverenigingen	2
Sociale Verzekeringsraad	0
Sociale fondsen	4
Uitvoeringsorganen sociale zekerheid overig	0
Overige dienstverlening	15
Kerkgenootschappen	0
Religieuze/levensbeschouwelijke org. Overig	0
Basisonderwijs	1
Middelbaar onderwijs	3
Hoger onderwijs	2
Schoolbegeleidings-/adviesdienst (SBD/SAD)	3
Universiteiten	13
Type- en computercursussen	0
Onderwijs overig	13
Ziekenhuizen	9

Psychiatrische Ziekenhuizen/inrichtingen	0
Verpleeghuizen	12
GG&GD	5
Bedrijfsgezondheidszorg (BGD's)	10
Revalidatiecentra	0
Bloedbanken	0
Kruiswerk/thuiszorg/kraamzorg	25
Medische instellingen overig	10
Huisartsenpraktijken	105
Overige artsen (niet specialisten)	0
Internist	0
Psychiater	1
Oogarts	3
KNO-arts	0
Dermatoloog	0
Zenuwarts	0
Overige specialisten-praktijken	7
Tandartsenpraktijken	15
Fysiotherapeuten	50
Mensendieck/Cesar	27
Pedicures/manicures/voetverzorging	191
Overige (para)medische behandelaars	170
Dierenartsen	0
Logopedisten	40
Diëtisten en voedingskundigen	8
Verloskundigen	8
Psychotherapeuten	38
Gezondheidszorg overig	68
Verzorgings- en bejaardentehuizen	19
Verblijven geestelijk/lichamelijk gehandic.	2
Sociaal-medische/psychologische/pedagog. dnst	7
Hulpinstellingen bij verslaving	0
RIAGG'S	1
Gezinsverzorging en gezinshulp	2
Vluchtelingenwerk	6
Dagverblijven voor kinderen	4
Relatiebemiddeling	33
Maatschappelijke dienstverlening overig	85
Buurt/clubhuis, jongeren/opbouw/vormingswerk	1
Bibliotheken	2
Arthoteken	0
Musea	0
Media	6
Sociaal-culturele-/culturele inst. overig	3
Sport en vrijetijdsbesteding	149
Kamers van Koophandel	30
Researchinstellingen	20
Publiekrechtelijke bedrijfsorganisaties	1
Vakbonden	2
Belangenverenigingen	19

Politieke partijen	0
Bedrijfs-/werknemersorganisaties overig	6
Begrafenis-, uitvaartondernemingen	2
Overige dienstverlening (overig)	28
Overig	0
Totaal	2289

Bijlage 2 Adviezen

Alle adviezen kunt u aanvragen bij de Registratiekamer of inzien op de website: www.registratiekamer.nl. Daarin zijn adviezen opgenomen vanaf 1996. U kunt de adviezen gratis afdrukken.

Adviezen vanaf 1991 zijn ook opgenomen in de bundel *Persoonsgegevens beschermd, Van WPR naar WBP*. Den Haag, Sdu uitgevers, 1999.

Advies paspoortwet

6 december 1999

Voorkomen dubbele inschrijvingen Koninkrijksdelen

22 oktober 1999

Advies besluit inlichtingen strafregisters

2 september 1999

Wijziging Wet op de Rechtsbijstand voor de verificatie van gegevens

31 augustus 1999

Wetsvoorstel invoering Sofi-nummer in de AWBZ

22 juli 1999

Advies SUWI-nota

9 juli 1999

Grondrechten in het digitale tijdperk

24 juni 1999

Gebruik sofi-nummer ter identificering verdachte

30 april 1999

Registratiekamer controle-autoriteit 'bijstand en samenwerking tussen douane-administraties

10 maart 1999

Voorgestelde regelgeving Vennoot '98 heeft aanpassing

5 maart 1999

Wet op de inlichtingen en -veiligheidsdiensten

2 maart 1999

Voorstel aanwijzing banken als informatieplichtig aan sociale diensten

19 januari 1999

Wetsvoorstel Wet bescherming persoonsgegevens

13 januari 1999

Bijlage 3 Onderzoeksrapporten

Alle onderzoeksrapporten kunt u aanvragen bij de Registratiekamer of inzien op de website: www.registratiekamer.nl. Daarin zijn onderzoeksrapporten opgenomen vanaf 1996. U kunt de onderzoeksrapporten gratis printen.

Controle e-mailverkeer door werkgever

27 december 1999

Verstrekken medische gegevens door werkgever

2 december 1999

Screeningsonderzoeken Bijzondere Opsporings Ambtenaar

6 april 1999

Is Landelijk Alcohol en Drugs Informatiesysteem een persoonsregistratie?

19 november 1999

Onderzoek naar handelsinformatiebureau Goderie van Groen

18 november 1999

Verstrekking van patiëntengegevens

9 september 1999

Uitbesteding taken Algemene Bijstandswet

8 september 1999

Gegevensverstrekking door gerechtsdeurwaarders

26 augustus 1999

Werken met gegevens - gegevensuitwisseling tussen CWI's en uitzendbureaus

augustus 1999

Bijstandsdoossiers en bescherming persoonsgegevens

10 juli 1999

Vastleggen en verstrekken van call detail records

24 juni 1999

Verzekeringsmaatschappij verplicht Arbo-dienst tot registratie en rapportage

14 juni 1999

Screening in Nederland

6 april 1999

Verstrekken van gegevens door deurwaarders

4 april 1999

Verdeling verantwoordelijkheden rond Donorregister

10 maart 1999

Geneeskundige registratie bij de Landmacht

1 maart 1999

Bijlage 4 Achtergrondstudies en Verkenningen

Alle publicaties in de serie Achtergrondstudie en Verkenningen kunt u aanvragen bij de Registratiekamer. U kunt de publicaties ook vinden op de website www.registratiekamer.nl. U kunt ze gratis afdrukken.

Zeeuw, J. de. *Informatieverstreking, Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving*. A&V-16, Den Haag, Registratiekamer. f 10.

Hes, R., Borking, J.J. en Hooghiemstra, T.F.M. *At face value. On biometrical identification and privacy*. A&V-15, Registratiekamer. f 10.

Artz, M.J.T. (1999) *Koning Klant. Het gebruik van klantgegevens voor marketingdoeleinden*. A&V-14, Registratiekamer. f 50.

Borking, J.J., e.a., *Intelligent software agents and privacy*, A&V-13, Registratiekamer 1999, f 40.

Hooghiemstra, T.F.M., *Privacy & Managed care*, A&V-12, Registratiekamer 1998, f 25.

Hes, R. en J. Borking, *Privacy-enhancing technologies: the path to anonymity*. revised edition. A&V-11, Registratiekamer 1998, f 25.

Almelo, L. van, e.a., *Gouden bergen van gegevens. Over datawarehousing, datamining en privacy*, A&V-10, Registratiekamer 1998, f 25.

Zandee, C., *Doelbewust volgen. Privacy-aspecten van cliëntvolgsystemen en andere vormen van gegevensuitwisseling*, A&V-9, Registratiekamer 1998, f 25.

Zeeuw, J. de, *Informatiegaring door de fiscus. Privacybescherming bij derdenonderzoeken*, A&V-8, Registratiekamer 1998, f 25.

Hulsman, B.J.P. en P.C. Ippel, *Gegeven: de Genen. Morele en juridische aspecten van het gebruik van genetische gegevens*, A&V-7, Registratiekamer 1996

Gardeniers, H.J.M., *Chipcards en privacy. Regels voor een nieuw kaartspel*, A&V-6, Registratiekamer 1995, f 25.

Rossum, H. van e.a., *Privacy-enhancing technologies: the path to anonymity, volume I and II* A&V-5, Registratiekamer 1995, f 50 (uitverkocht).

Rommelse, A.F., *Zwarte lijsten. Belangen en effecten van waarschuwingssystemen* A&V-4, Registratiekamer 1995, f 25.

Rommelse, A.F., *Ziekteverzuim en privacy. Controle door de werkgever en verplichtingen van de werknemer A&V-3*, Registratiekamer 1995 f 25.

Casteren, J.P.M. van, *Bevolkingsgegevens: Wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden A&V-2*, Registratiekamer 1995 (uitverkocht)

Rossum, H. van e.a., *Beveiliging van persoonsregistraties*, Registratiekamer 1994, f 25.

Overige publicaties

Stratum M. van, *Tegen het licht gehouden, verslag van de rondetafelconferentie over screening in Nederland*. Den Haag, 1999.

Persoonsgegevens beschermd. Uitspraken van de Registratiekamer, Sdu Uitgevers, Den Haag 1999, f69

Bibob on trial, Verslag meeting Bevordering integere besluitvorming openbaar bestuur. Den Haag, Registratiekamer, 1998, f 25

Vries H.H. de, met J.H.J. Terstegge (red.), *De werknemer achtervolgd? Over personeelsvolgsystemen, verzuimcontrole en de nieuwe bevoegdheden van de OR*, Sinzheimer Cahiers 14, SDU, Den Haag 1998.

Ippel, P., e.o. (ed), *Privacy disputed*, Registratiekamer 1995, f 40

Proceedings of the 16th International Conference on Data Protection, The Hague 1994 - Facing Dilemmas Registratiekamer 1995, f 25.

Hoever laat de student zich in de kaart kijken? Symposium over chipcards en privacy, Registratiekamer/Informatie Beheer Groep 1997.

Bijlage 5 Brochures en Informatiebladen

Brochures en informatiebladen kunt aanvragen bij de Registratiekamer. U vindt ze ook op de website www.registratiekamer.nl.

De Wet persoonsregistraties - de bescherming van uw persoonlijke gegevens, Registratiekamer 1999.

De Wet politieregisters - uw gegevens bij de politie, Registratiekamer 1996.

Registratiekamer, Registratiekamer 1999.

Een zekere privacy - Beveiliging van gegevens over uw personeel, leden, abonnees, klanten en andere relaties, Registratiekamer 1995.

In vertrouwen gegeven - Uitgangspunten, regels en praktijkvoorbeelden voor het werken met persoonsgegevens, Registratiekamer 1996.

Informatiebladen

Uw klacht en de Registratiekamer, Registratiekamer 1999

Bemiddeling door de Registratiekamer, Registratiekamer 1999

Het toetsen van uw kredietwaardigheid, Registratiekamer 1999

Het gebruik van kentekengegevens en uw privacy, Registratiekamer 1999

Camera's op de werkplek, Registratiekamer 1999

Doorgeven van personeelsgegevens, Registratiekamer 1999

Geadresseerde reclame, Registratiekamer 1999

Bijlage 6 Publicaties in vakbladen en tijdschriften 1998

Berichten van de Registratiekamer in Privacy & Informatie, februari/april/juni/ augustus/ oktober/december 1999, Sdu uitgeverij, 1999.

Alonso Blas, D. **25 oktober 1998: The day after** in Privacy en Informatie, nr. 1, februari 1999.

Alonso Blas, D., **Privacy wetgeving in Europa, Europa in beweging** in Magazine EBN, nr. 6, december 1999.

Alonso Blas, D., Hyland, M. and Dumortier, J. **Advanced Security for Personal Communications Technologies**. Legal Issues, Final report, Deliverable 25, AC095/KUL/W26/ DS/P/25/1, Aspect project, ICRI, K.U. Leuven, 1999

Alonso Blas, D. en Zeeuw, J. de, **Proteccion de datos y pago de peajes. Uso de nuevas tecnologias para la vigilancia de carreteras**. Novatica, enero/febr. 1999, no. 137, 69-73.

Borking, J.J. and Verhaar, P. **Biometrie und Datenschutz, Bedrohungen und privacy-enhancing technologies** in DUD (Datenschutz und Datensicherheit) no. 3/1999, p. 138-142.

Borking J.J., **Data warehousing en data mining** in Informatiebeveiliging jaarboek 1999/2000.

Hes, R. en Hooghiemstra, T.F.M., **Biometrische identificatie** in Informatiebeveiliging Praktijkjournaal, nr. 6, augustus 1999.

Hes, R., **Software agents: slaven of meesters?** in Informatiebeveiliging Praktijkjournaal, Ten Hagen Stam, nr. 7, september 1999.

Hes, R., **Cryptografie ontsleuteld** in Informatiebeveiliging Jaarboek 1999/2000, Ten Hagen Stam, p. 67-75.

Hooghiemstra, T.F.M., **De WBP en de gezondheidszorg** in Tijdschrift voor gezondheidsrecht, 1999, nr. 1, p. 17-27.

Hooghiemstra, T.F.M., **Gouden bergen in de gezondheidszorg, een beschouwing over datamining, managed care en privacy** in Privacy & Informatie, nr. 3, juni 1999, p. 115-118.

Hustinx, P.J., **Interventie** in Wetgeving voor de elektronische snelweg: nadere beschouwingen, H. Hijmans en A. de Kroon (red.), ITeR-reeks, nr. 16, Kluwer, Deventer 1999, p. 61-63.

Hustinx, P.J., **Bescherming privacy in de lidstaten van de Europese Unie** in Privacy, Seminarie Egmontpaleis, Brussel 1999, p. 36-44.

Hustinx, P.J., **Veranderingen in de Privacywetgeving**, Studiedag 'De Nieuwe Privacywet en de Geo-informatiesector', Utrecht, 25 maart 1999

Hustinx, P.J., **Informatietechnologie in de gezondheidszorg**, preadvies voor de Vereniging voor Gezondheidsrecht, Jaarvergadering, 23 april 1999.

Hustinx, P.J., **Het gebruik van privacygevoelige gegevens**, Vakblad Financiële Planning, mei 1999, p. 7-10.

Hustinx, P.J., **Nederland moet Europese privacyrichtlijn volgen**, NRC Handelsblad, 23 augustus 1999.

Hustinx, P.J., **Data Protection** in Who owns our genes?, Conference 15-17 October 1999, Tallinn, Estonia, organised by Nordic Committee on Bioethics.

Linden, A. ter, **Checklist voor medische chipcards. Een checklist om een chipcardproject een kans van slagen te geven** in Privacy & Informatie, september 1999.

Pol, U. van de, **Bliksemafleider**. gastcolumn in Algemeen politieblad, 30 januari 1999

Pol, U. van de en Leur, A. van de, **Maathouden bij invoering cameratoezicht** in Algemeen politieblad 1999, blz.4-6.

Pol, U. van de en Heij, G. de, **Anonimisering van jurisprudentie** in Trema 199, blz. 260-265.

Pol, U. van de, **Privacy in democratische rechtsstaat**, bespreking van S. Gutwirth, privacyvrijheid, in Mediaforum 1999, blz. 105-108.

Pol, U. van de, Beroepscommissie Centrale Raad voor Strafrechtstoepassing 21 juli 1998, **Verstrekking uit persoonsdossier**, annotatie in Sancties 1999, 1.

Stratum, M. van en Pol, U. van de, **Screening op integriteit, Bibob gewogen en te licht bevonden** in Nederlands Juristen Blad, november 1999.

Terstegge, J.H.J., **Personeelsinformatiesystemen en de privacywetgeving** in Handboek Methoden, Technieken en Analyses voor Personeelsmanagement (losbladig). Aflevering 55 (I.6.2.2-7), december 1999, Samsom, Deventer, p. 701-724.

Terstegge, J.H.J., **Zieke werknemers en het recht op privacy-ziekteverzuim en controle** in Privacy & Informatie, oktober 1999, nr. 5, p. 212 - 217.

Terstegge, J.H.J., **Zijn uw PI-systemen WBP-proof?** in Praktijkblad Arbeidsvoorwaarden Januari/februari 1999, nr.1-2, p.9-11.

Vries, H.H de, **(Verborgen) cameratoezicht op de werkplek** in Privacy & Informatie, nr. 6, december 1999, p. 256-263..

Vries, H.H. de, **Noot bij EHRM 25 juni 1997 (Halford)** in SMA 1999, 4, p. 207-212.

Vries, H.H. de, **Privacy: gloort er licht aan het einde van de tunnel?** in Sociaal Recht, juni 1999, p. 151-152.

Gedragscodes waarvoor de Registratiekamer een Verklaring van Overeenstemming heeft verleend

Gedragscode verwerking persoonsgegevens verzekeringsbedrijf (Verbond van Verzekeraars), geldig tot 5 maart 2001 (Stcrt. 1998, 44)

Privacy Gedragscode van de Nederlandse Vereniging van Banken; geldig tot 16 oktober 1998 (Stcrt. 1995,207)

Gedragscode Gezondheidsonderzoek van de Federatie van Medisch Wetenschappelijke Verenigingen; geldig tot 14 juli 2000; (Stcrt. 1995,140)

Gedragscode van de Nederlandse Vereniging van Handelsinformatiebureaus; geldig tot 25 juni 1998; (Stcrt. 1993,118)

Privacy Gedragscode van de Nederlandse Postorderbond; geldig tot 1 april 1996 (Stcrt. 1993,60)

Gedragscode van de Vereniging van Fabrikanten en Importeurs van Diergeneesmiddelen in Nederland (FDIN); geldig tot 3 december 1997, (Stcrt. 1992,235)

Gedragsregels in verband met de bescherming van de persoonlijke levenssfeer van de Nederlandse Associatie van de Farmaceutische Industrie (Nefarma), geldig tot 13 oktober 1997 (Stcrt. 1992,198)

Gedragscode Direct Marketing Instituut Nederland; geldig tot 2 oktober 1995 (Stcrt. 1992,194)

Privacy-gedragscode van de Vereniging van Marktonderzoekbureaus en de Nederlandse Vereniging van Marktonderzoekers, geldig tot 12 juni 1996 (Stcrt. 1991,111)

Gedragscode persoonsregistraties van de Vereniging van Onderzoeks Instituten in gedrags- en maatschappijwetenschappen, geldig tot 8 mei 1996, (Stcrt. 1991,88)

Gedragscode persoonsregistraties van de Branchevereniging voor Informatietechnologie COSSO; geldig tot 17 januari 1994 (Stcrt. 1991,12)

Privacy Code van de Organisatie van Adviesbureaus voor Werving en Selectie (OAWS), geldig tot 28 november 1995 (Stcrt. 1990,232)

Bijlage 8 Modelreglementen vastgesteld voor politieregisters

Modelreglementen vastgesteld voor politieregisters

Aandachtsvestigingen (Stcrt. 1994,78)
Advertentie
Arrestanten (Stcrt. 1994,78)
Arrestatiebevelen (Stcrt. 1994,78)
Bedrijfsprocessensysteem BPS (Stcrt. 1994,78)
Bedrijven informatiesysteem en Waarschuwingsadressen (Stcrt. 1994,78)
Bekeuringenafhandelingssysteem (Stcrt. 1994,78)
Beperkingen Besturen Motorrijtuigen (Stcrt. 1994,78)
Bureau Financiële Ondersteuning (Stcrt. 1996,125)
Criminele Inlichtingendienst (Stcrt. 1993,182)
Fraudebestrijding (Stcrt. 1994,78)
Gevonden en verloren goederen (Stcrt. 1994,78)
Graffitibestrijding (Stcrt. 1994,78)
Grijze-veld (Stcrt. 1993,182)
Herkenningdienst (Stcrt. 1994,78)
Inbeslaggenomen goederen (Stcrt. 1994,78)
Inbraakbestrijding (Stcrt. 1994,78)
In bewaring genomen goederen (Stcrt. 1994,78)
Internationale rechtshulp politie (Stcrt. 1994,144)
Jeugd- en zedenzaken (Stcrt. 1994,78)
Kabinetszaken (Stcrt. 1994,78)
Meldkamer (Stcrt. 1994,78)
Milieudelicten (Stcrt. 1994,78)
Multipol (Stcrt. 1994,78)
Openbare orde Regionale inlichtingendienst (Stcrt. 1996,125)
Opkopers en Helingbestrijding (Stcrt. 1994,78)
Overvallenbestrijding (Stcrt. 1994,78)
Permanent Autoteam (Stcrt. 1994,78)
Processen-verbaal en rapporten (Stcrt. 1994,78)
Recidive (Stcrt. 1994,78)
Rijverboden (Stcrt. 1994,78)
Schietwapen incidentenregistratie en informatiesysteem (Stcrt. 1994,78)
Technische recherchezaken (Stcrt. 1994,78)
Vakantiecontrolekaarten (Stcrt. 1994,78)
Vandalismebestrijding (Stcrt. 1994,78)
Verdovende middelen (Stcrt. 1994,78)
Wijziging Herkenningdienst (Stcrt. 1996,125)

Bijlage 9 Documenten van de Werkgroep inzake de bescherming van persoonsgegevens (artikel 29 van Richtlijn 95/46/EG)

3 December 1999 – **Opinion 7/99 on the Level of Data Protection provided by the “Safe Harbor” Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce** (Document 5146/99 - WP 27)

7 September 1999 – **Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights** (Document 5143/99 - WP 26)

7 September 1999 – **Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes** (Document 5085/99 - WP 25)

7 September 1999 – **Opinion 6/99 concerning the level of personal data protection in Hungary** (Document 5070/99 - WP 24)

7 July 1999 – **Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the “International Safe Harbor Principles”** (Document 5075/99 - WP 23)

7 June 1999 – **Opinion 5/99 on the level of protection of personal data in Switzerland** (Document 5054/99 - WP 22)

7 June 1999 – **Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed “Safe Harbor Principles”** (Document 5066/99 - WP 21)

3 May 1999 – **Opinion 3/99 on public sector information and the protection of personal data** (Document 5026/99 - WP 20)

3 May 1999 – **Opinion 2/99 on the Adequacy of the “International Safe Harbor Principles” issued by the US Department of Commerce on 19th April 1999** (Document 5047/99 - WP 19)

3 May 1999 – **Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications** (Document 5005/99 - WP 18)

23 February 1999 – **Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware** (Document 5093/98 - WP 17)

23 February 1999 – **Working Document: Processing of Personal Data on the Internet** (Document 5013/99 - WP 16)

26 January 1999 – **Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government** (Document 5092/98 - WP 15)

Zie ook: <http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index>.

Bijlage 10 Formatie 1995-1998

Formatie per 31 december uitgedrukt in volledige arbeidsplaatsen (fte)

	1996	1997	1998	1999
beschikbaar	39,4	41,4	43	49,4
bezet	37,9	37,8	41,5	47,9
aantal medewerkers	42	43	47	52

Bijlage 11 Activiteiten 1996-1999 in cijfers

	1996	1997	1998	1999
Adviezen aan regering en parlement	18	27	18	21
Onderzoeksrapporten	10	7	9	16
Achtergrondstudies en Verkenningen	1		6	4
Overige publicaties	1	1	1	1
Klachten en geschillen	245	374	319	276
Telefonisch spreekuur	4720	4970	5500	6763
Aanmeldingen	55601	57786	61111	2289

Colofon

Uitgave: Registratiekamer
Afdeling Communicatie
Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag
telefoon 070-3811300
telefax 070-3811301
mail@registratiekamer.nl

Samenstelling & eindredactie: Diana Alonso Blas
en Rudy Schreijnders

Fotografie: ?

Vormgeving: Miriam Monster (plan: Information design)

Met bijzondere dank aan: Marijn Artz, Erik Bogaards, Mirjam Hazenoot, Ronald Hes,
Theo Hooghiemstra, Bernard Hulsman, Michel van Stratum,
Koen Vermissen, Henk van der Wel en Carine Zandee.