Jaarverslag 1998

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

www.registratiekamer.nl

mei 1999

Registratiekamer

Om te bevorderen dat de privacy van de burger voldoende is gewaarborgd en dat de wetten die daartoe zijn vastgesteld worden nageleefd, is in 1989 de Registratiekamer ingesteld als onafhankelijk toezichthouder. De Registratiekamer adviseert de regering over beleid en wetgeving waarin de privacy van de burger in het geding is. Zij toetst gedragscodes die door organisaties binnen een bepaalde sector worden vastgesteld over het gebruik van persoonsgegevens. Zij verricht studies en stelt onderzoeken in naar de inrichting en het gebruik van persoonsregistraties. Zij behandelt klachten over het gebruik van persoonsgegevens en bemiddelt in geschillen hierover tussen burgers en organisaties. Tenslotte vertegenwoordigt de Registratiekamer Nederland in internationale overleg- en controleorganen op het gebied van privacybescherming. De Registratiekamer wil in het denken over, het ontwikkelen van en het communiceren over relevante normen ten aanzien van de informationele privacybescherming een voor de samenleving herkenbare en onbetwiste leider zijn. Zij bevordert en bewaakt de toepassing van deze normen en bepaalt daardoor mede het humane gezicht van de informatiesamenleving van de 21ste eeuw.

Om haar taak als toezichthouder effectief te vervullen, heeft de Registratiekamer gekozen voor de strategie langs vier sporen -bewustwording, normontwikkeling, technologie en handhaving- de bescherming van persoonsgegeven te bevorderen. Met voorlichting en met 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 uitgewerkt en geïnterpreteerd naar verschillende contexten. 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.

Ten geleide

In dit jaarverslag vindt u een overzicht van de activiteiten en producten van de Registratiekamer over het jaar 1998. Het overzicht is beknopter dan voorheen en ook anders samengesteld. De belangrijkste reden voor deze nieuwe opzet is dat inmiddels verschillende andere bronnen beschikbaar zijn waaruit informatie kan worden geput over de activiteiten en producten van de Registratiekamer: het katern 'Berichten van de Registratiekamer' in het tijdschrift *Privacy & Informatie*, de uitsprakenbundel *Persoonsgegevens beschermd* en de website van Registratiekamer: www.Registratiekamer.nl. Het jaarverslag bevat nu een beknopt overzicht en een drietal hoofdstukken over de belangrijkste thema's van 1998. In hoofdstuk 1 wordt in vogelvlucht een impressie gegeven van de activiteiten van de Registratiekamer in 1998. In de hoofdstukken 2, 3 en 4 vindt u een bespreking van drie thema's waaraan de Registratiekamer in 1998 veel aandacht heeft besteed en waarvan zij verwacht 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 de strategie van de vier sporen. Overzichten van aangemelde persoonsregistraties, uitgebrachte adviezen, onderzoeksrapporten en achtergrondstudies, gepubliceerde artikelen en overige gegevens, vindt u in de bijlagen.

mr. P.J. Hustinx (voorzitter)
drs. J.J. Borking (lid)
dr. U. van de Pol (lid)

Inhoud

1 1998 in vogelvlucht

De invoering van de nieuwe Wet bescherming persoonsgegevens laat langer op zich wachten dan voorzien. Maar met de voorbereiding op die invoering is de Registratiekamer in 1998 al begonnen. De bescherming van persoonsgegevens in de financiële sector, waarbinnen zich grote conglomeraten vormen en waarin de stroom van persoonsgegevens steeds intensiever wordt, is in 1998 op de agenda gezet. De eerste stappen zijn gezet voor een gezamenlijk onderzoek van vijf toezichthouders die hierin hun eigen verantwoordelijkheid hebben: De Nederlandsche Bank, de Verzekeringskamer, het College van toezicht sociale verzekeringen, de Ziekenfondsraad en de Registratiekamer (zie hoofdstuk 2). Aan de gevolgen van de privatisering van de uitvoering van de sociale zekerheid voor de privacy van werknemers en werkzoekenden is in het verslagjaar opnieuw veel aandacht besteed, onder meer met een advies aan de regering (zie hoofdstuk 3). De parlementaire behandeling van de Telecommunicatiewet was de gelegenheid voor de Registratiekamer om haar standpunt uiteen te zetten over de handhaving van de vertrouwelijkheid en anonimiteit in de verschillende vormen van telecommunicatie (zie hoofdstuk 4).

Plannen van gemeentelijke overheden om het niet-gebruik van huursubsidie en andere sociale voorzieningen te reduceren, hebben geleid tot adviezen van de Registratiekamer aan de minister van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer en de minister van Sociale Zaken en Werkgelegenheid en een nauwe betrokkenheid bij de opzet van pilot-projecten in Groningen, Alphen a/d Rijn en Den Haag. Ontwikkelingen in de gezondheidszorg, de introductie van *managed care* en de uitwisseling van gegevens tussen hulpverleners en zorgverzekeraars, zijn reden geweest voor overleg met de betrokken partijen en de ontwikkeling van een kader waarbinnen de privacy van de patiënt veilig wordt gesteld. De invoering van het onderwijsnummer -waarover de Registratiekamer in 1996 haar eerste advies uitbracht- was in 1998 nog steeds onderwerp van discussie. De Registratiekamer heeft aan het parlement (opnieuw) aangegeven wat de haken en ogen zijn.

Een onderzoek naar de bevoegdheden van de belastingdienst om gegevens te verzamelen is afgesloten met de publicatie *Informatiegaring door de fiscus*, waarin de Registratiekamer concludeert dat de wettelijke bevoegdheden verder gaan dan nodig is. *Datawarehousing en datamining* vinden op steeds meer terreinen, in de publieke en in de private sector, hun toepassing. In de publicatie *Gouden bergen van gegevens* heeft de Registratiekamer de juridische voorwaarden aangegeven waaronder dergelijke methoden en technieken aanvaardbaar zijn. Samenwerking in de jeugdhulpverlening en nauwe begeleiding van probleemjongeren leidt tot uitwisseling van persoonsgegevens tussen verschillende instanties. De bescherming van persoonsgegevens in cliëntvolgsystemen was het onderwerp van een studie die in 1998 leidde tot de publicatie *Doelbewust volgen*. De inzet van videocamerasystemen voor beveiliging en bewaking wint alleen maar aan populariteit en was ook in dit verslagjaar een terugkerend onderwerp op de agenda.

De Registratiekamer heeft bijgedragen aan de modernisering van het Verdrag van Straatsburg van 1981 en in het kader van de werkgroep ex artikel 29 van Richtlijn 95/46/EG deelgenomen aan de discussie over de implementatie van de Europese richtlijn en het gegevensverkeer met derde landen. Op uitnodiging heeft de Registratiekamer over dit laatste onderwerp ook in de Verenigde Staten overleg gevoerd.

2 Bescherming van persoonsgegevens in de financiële sector

De Registratiekamer heeft in 1998 het gesprek geopend met De Nederlandsche Bank (DNB), de Verzekeringskamer, het College van toezicht sociale verzekeringen (CTSV) en de Ziekenfondsraad over de mogelijkheden om gezamenlijk een onderzoek in te stellen naar het informatiemanagement en de verwerking van gegevens in financiële conglomeraten. Doel van een dergelijk onderzoek is de inzichtelijkheid van het informatiemanagement te bevorderen en een taxatie te maken van de integriteit van het gegevensverwerkend proces. Er zijn geen aanwijzingen dat er op dit gebied sprake is van structurele misstanden, maar het is beter om feitelijk te kunnen vaststellen dat een zorgvuldig en behoorlijk gebruik van persoonsgegevens in de financiële sector is gewaarborgd. Bij de financiële diensten van banken, verzekeraars en soortgelijke instellingen gaat het immers niet alleen om geld, maar ook om veel gegevens: over cliënten, hun mogelijkheden en wensen, over toekomstige cliënten en over ongewenste risico's. Met de opkomst van nieuwe diensten, elektronische media, schaalvergroting en privatisering wordt dat alleen maar aangewakkerd. Het vertrouwen dat met die gegevens zorgvuldig, behoorlijk en integer wordt omgegaan, wordt niet alleen voor de betrokken instellingen zelf, maar ook voor hun cliënten en relaties steeds meer een factor om rekening mee te houden. Een zorgvuldig gegevensmanagement, waarin de zorg voor de privacygevoelige gegevens van cliënten is verankerd, zal dus ook steeds meer een voorwaarde moeten worden voor integere financiële dienstverlening en op een adequate wijze moeten worden gewaarborgd.

Vertrouwen

Er zijn maar weinig financiële diensten waarbij de gegevens van cliënten niet vroeg of laat een rol spelen. Een bankrekening openen is zonder identiteitsvaststelling niet mogelijk. Met het gebruik van de rekening worden gegevens zichtbaar over inkomsten en vermogen, bestedingen, eigenschappen en gewoonten. Ook als de bank daarvoor geen belangstelling heeft en zich alleen ziet als de uitvoerder van de opdrachten van de cliënt, raakt zij daarbij toch betrokken als houder van de bankadministratie waarlangs het verkeer van financiële diensten verloopt. Steeds vaker zullen banken, credit card-maatschappijen en andere bij de afwikkeling van het betalingsverkeer betrokken instellingen wel belangstelling hebben voor dergelijke gegevens, omdat zij bruikbaar zijn bij het ontwikkelen, aanbieden en beheren van nieuwe diensten. Het anticiperen op de wensen van de cliënt is even interessant als het voorkomen van ongewenste risico's of het op peil houden van het rendement. Naarmate het dienstenpakket van de bank breder of gevarieerder is, zal zij meer inzicht krijgen en meer in staat zijn selecties te maken. Bij risicovolle transacties zal zij ook meer willen weten van de persoonlijke of zakelijke omstandigheden die voor de beoordeling van de transactie relevant zijn.

Sinds mensenheugenis hebben bankiers een vertrouwenspositie: het vertrouwen van cliënten in de deugdelijkheid van de dienstverlening, maar ook in de zorg waarmee de aldus verkregen gegevens worden beheerd, is in deze bedrijfstak een belangrijk uitgangspunt waaraan veel aandacht wordt besteed. Een bankgeheim zoals enkele andere landen kennen, bestaat in Nederland niet. Wel is het zo dat banken anders dan vroeger bijvoorbeeld geen handelsinformatie meer aan derden verstrekken, tenzij met voorafgaande schriftelijke toestemming van de betrokken cliënt. Wettelijke informatieplichten, zoals aan de fiscus of

krachtens de Wet melding ongebruikelijke transacties, staan in de huidige praktijk tegenover een stringente geheimhoudingsplicht van DNB. Het toezicht van DNB lijkt vooral gericht op de financiële soliditeit.

Bij de verzekeraars is het beeld in essentie niet anders. Nog meer dan bankieren is verzekeren een kwestie van vertrouwen. Bij het aangaan van een verzekering zal een cliënt informatie moeten verstrekken over het te dekken risico. De verzwijging van relevante informatie kan leiden tot nietigheid van de verzekering. Bij de verzekering van bepaalde risico's zoals ziekte of overlijden, zullen medische gegevens op tafel moeten komen, in het geval van een ziektekostenverzekering zelfs gedurende de hele looptijd. Verzekeraars hebben door de aard van hun bedrijf soms een vergaand inzicht in de persoonlijke omstandigheden van hun cliënten. Een positie die zelfs kan leiden tot inzicht in ziektepatronen binnen families die kunnen wijzen op een erfelijke aanleg. Ook verzekeraars hebben daarom belang bij een stevig vertrouwen van hun cliënten in de wijze waarop zij met dergelijke gevoelige gegevens omgaan. Met het gevarieerder worden van het aanbod aan verzekeringsproducten staan echter ook verzekeraars steeds vaker voor de vraag of de bijzondere kennis die zij uit hoofde van een bepaald contract hebben opgedaan, ook mag worden gebruikt voor het doen van aanbiedingen of risicoselectie in een ander kader. Bij het toezicht op de betrouwbaarheid van verzekeraars, in hoofdzaak ondergebracht bij de Verzekeringskamer, lijkt financiële soliditeit, net als in de bancaire sector, echter nog steeds op de voorgrond te staan.

Wat geldt voor de verzekeraars, geldt in principe ook voor de tussenpersonen in deze sector. Ook die zijn in steeds wisselende combinaties betrokken bij het afwikkelen van een veelheid aan financiële transacties. Hoe staat het met de gegevens over persoonlijke omstandigheden die hun uit hoofde van die transacties ter kennis komen? En wat geldt voor een bank die tevens optreedt als tussenpersoon voor een verzekeraar? Dergelijke vragen nemen in aantal toe en worden klemmender, naarmate de betrokken branches verder met elkaar verknoopt raken.

Wet en zelfregulering

Hoe kan een cliënt, consument of werknemer er op rekenen dat de persoonlijke gegevens die hij voor legitieme doeleinden met anderen deelt, in de praktijk alleen voor die doeleinden worden gebruikt? In hoeverre kan hij dat gebruik zelf bepalen of tenminste zicht houden op wat er met zijn gegevens gebeurt? De regels daarvoor zijn in wetgeving neergelegd. De Wet persoonsregistraties van 1989 zal waarschijnlijk in 1999 worden vervangen door de Wet bescherming persoonsgegevens (WBP). De WBP zal, net als de huidige WPR, een aantal dwingende normen stellen waaraan alle instanties die persoonsgegevens met computers of in gestructureerde bestanden verwerken, zullen zijn gebonden. Dat geldt dus ook voor banken, verzekeraars en andere financiële instellingen. Eén van deze normen houdt in dat de betrokken personen vooraf moeten kunnen weten voor welke doeleinden gegevens over hen worden verzameld en vastgelegd. Een andere norm houdt daarmee direct verband, namelijk dat gegevens – enkele uitzonderingen daargelaten – alleen mogen worden gebruikt voor doeleinden die verenigbaar zijn met de doeleinden waarvoor zij zijn verkregen. Afgezien van deze algemene normen, zullen betrokkenen vaker dan nu zelf invloed kunnen uitoefenen op de verwerking van hun gegevens. De Registratiekamer, nu onder meer belast met het toezicht op de naleving van de WPR, zal College bescherming persoonsgegevens (CBP) gaan heten en meer bevoegdheden krijgen om de naleving van de nieuwe wet indien nodig af te dwingen. In

de opzet van de WBP is dat een uiterste middel. Binnen de algemene normen van de wet is veel ruimte gelaten voor nadere invulling en concrete uitwerking door middel van zelfregulering. Daarbij valt te denken aan de ontwikkeling van gedragscodes voor bepaalde branches, al dan niet met de mogelijkheid van geschillencommissies.

Zelfregulering via gedragscodes vormt ook in de WPR een belangrijk element. Sinds 1989 zijn inmiddels twaalf gedragscodes voor uiteenlopende branches door de Registratiekamer goedgekeurd. Twee van die gedragscodes zijn hier relevant, namelijk de Privacy Gedragscode Banken (Stcrt. 1995, 207) en de Gedragscode Verwerking Persoonsgegevens Verzekeringsbedrijf (Stcrt. 1998, 44). De laatste van deze twee is nu het meest interessant, omdat daarin al expliciet wordt vooruitgelopen op de WBP om een soepele overgang op de nieuwe wettelijke regeling mogelijk te maken. Interessant ook, omdat in deze gedragscode uitvoerig aandacht wordt besteed aan de problematiek van de gegevensuitwisseling en het verenigbaar gebruik in concernverband. Hierbij rijst de vraag in hoeverre persoonsgegevens die door een verzekeringsinstelling zijn verkregen, ook gebruikt mogen worden voor of door andere tot het concern behorende rechtspersonen.

In de toelichting wordt opgemerkt dat de vraag wanneer sprake is van onverenigbaar gebruik, onder de Europese richtlijn en de WBP een wijdere strekking heeft. Dat gegevens niet mogen worden verwerkt op een wijze die onverenigbaar is met het doel waarvoor ze zijn verzameld, is een norm die onder de WBP betrekking zal hebben op iedere verwerking van persoonsgegevens binnen of buiten de organisatie van het betrokken bedrijf. Bij de vraag of een bepaalde voorgenomen verwerking van persoonsgegevens verenigbaar is met het doel waarvoor die gegevens zijn verzameld, is een aantal criteria van belang: de verwantschap tussen het doel van de verwerking en het doel waarvoor de gegevens zijn verkregen; de aard van de betreffende gegevens; de gevolgen van de verwerking voor de betrokkene; de wijze waarop de gegevens zijn verkregen; en de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen. Hoewel deze criteria inmiddels zijn geschrapt uit het voorstel voor de WBP, ligt de toepassing daarvan bij de invulling van ‘verenigbaar gebruik’ nog steeds voor de hand.

Of en in hoeverre een verzekeringsconcern of financieel conglomeraat in het kader van haar activiteiten tot gegevensuitwisseling zal kunnen overgaan, dient van geval tot geval te worden beoordeeld aan de hand van de hiervoor weergegeven criteria. De toelichting noemt daarvan enige voorbeelden. In het algemeen wordt toelaatbaar geacht dat de enkele informatie dat een uitkering onder een schadeverzekering is verschuldigd, toegankelijk is voor onderdelen van de groep waartoe de verzekeringsinstelling behoort om het beleid met betrekking tot elders in het concern bestaande vorderingen op de betrokkene te kunnen bepalen. De aan de uitkering ten grondslag liggende gegevens zullen in het algemeen echter niet voor andere onderdelen van het concern beschikbaar mogen zijn. Als schoolvoorbeeld van verwantschap tussen de afgenomen en aangeboden diensten wordt het geval genoemd van de hypotheekbank die naar aanleiding van hypothecaire leningen een schadeverzekeraar attendeert op de mogelijkheid een mailing over aangeboden opstalverzekeringen te verzenden. Een ziektekostenverzekeraar mag echter niet op basis van het claimgedrag van zijn verzekerden een selectie toepassen en de resultaten van die selectie doorgeven aan een arbeidsongeschiktheidsverzekeraar. Dergelijk gebruik is in de code dan ook uitgesloten. Medische gegevens die zijn verwerkt met het oog op de beoordeling van een te verzekeren risico of bij de uitvoering van een overeenkomst, mogen zonder toestemming van de betrokkene niet worden gebruikt in een ander kader.

De hiervoor geschetste benadering van het verzekeringsbedrijf leent zich voor een bredere toepassing. Overgebracht op de vraag in hoeverre de gegevens die beschikbaar komen bij de afwikkeling van het betalingsverkeer via een bank of credit card-maatschappij, voor andere doeleinden mogen worden gebruikt, zou het resultaat wel eens kunnen zijn dat uitwendige feiten over betalingsgedrag, zoals tijdstip en wijze van betaling, op een andere wijze moeten worden behandeld dan gegevens die voortvloeien uit een analyse van betalingsgedrag. De eerste groep van gegevens raakt de bedrijfsvoering van de instelling rechtstreeks, terwijl bij de tweede groep een veel grotere terughoudendheid past, omdat die gegevens nu eenmaal als onvermijdelijk uitvloeisel van de betaaldienst aan de instelling zijn toevertrouwd.

Nabije toekomst

Wie aan de hand van het hiervoor geschetste kader de toekomst beziet, zal zich in elk geval op een aantal ontwikkelingen moeten beraden. De elektronische betaling met betaalpassen en credit cards, al dan niet in de vorm van chipcards, zal zodanig moeten zijn ingericht dat het primaire doel van de transactie zo efficiënt en veilig als mogelijk is wordt gerealiseerd. Secundaire doelen die de klant niet bekend zijn gemaakt of waartegen deze op goede gronden bezwaar heeft, zullen liefst ook technisch onmogelijk moeten worden gemaakt. Het gebruik van chipcards is ook actueel in de sfeer van de ziektekostenverzekeraars, die voorbereidingen treffen voor de grootschalige invoering van zorgpassen. De Registratiekamer beziet in overleg met Zorgverzekeraars Nederland aan welke voorwaarden deze zorgpassen voor een efficiënte en veilige afwikkeling van betalingen in de gezondheidszorg moeten voldoen. Daarbij wordt ook in kaart gebracht welk gebruik nu wordt gemaakt van de declaratiegegevens. Het is de bedoeling dat deze exercitie leidt tot een annex bij de gedragscode voor het verzekeringsbedrijf, waarin de bijzondere spelregels op dit terrein worden neergelegd.

In 1998 heeft de Registratiekamer een rapport uitgebracht over datawarehousing, datamining en privacy onder de titel *Gouden bergen van gegevens* (Achtergrondstudies & Verkenningen nr. 10). Tegen de achtergrond van de Europese richtlijn en de WBP, wordt in deze publicatie aangegeven welke regels van privacybescherming van belang zijn voor datawarehousing en datamining. In het rapport komt ook de toepassing van deze technieken in de financiële sector aan de orde. Het aanleggen van een datawarehouse leidt tot het bijeenbrengen van gegevens over cliënten uit verschillende bronnen. De eerder besproken regels over gegevensverkeer en verenigbaar gebruik in concernverband worden daarbij op de proef gesteld. Dat kan een reden zijn om het ‘datawarehouse’ zo in te richten dat daarin geen persoonsgegevens voorkomen dan onder zeer nauwkeurig omschreven voorwaarden, die in de opzet en werking van het systeem zijn terug te vinden. In het rapport worden suggesties hiervoor gedaan die berusten op de inzet van ‘privacy enhancing technologies’ (PET), waarmee de ‘zachte normen’ van de privacywetgeving kunnen worden vertaald in ‘harde systeemeisen’ en waarbij vaak gebruik wordt gemaakt van encryptie. Met NCR, marktleider in de wereld op het gebied van zeer grote databases, heeft de Registratiekamer op dit punt vruchtbare contacten gelegd. Dit bedrijf heeft privacybescherming voor zichzelf al enkele jaren geleden als strategische *business opportunity* gedefinieerd. Dergelijke stappen zijn de komende tijd ook van andere spelers op het terrein van *electronic commerce* te verwachten.

De belangen die aan de orde zijn, zijn zonder enige twijfel van groot gewicht, zowel politiek, maatschappelijk en economisch, als voor de betrokkenen persoonlijk. Het vermogen om als individu in een elektronische omgeving, vrije keuzes te maken, met voldoende zicht op de

consequenties en de redelijke zekerheid dat de werkelijkheid daarmee zal sporen, raakt een essentieel kenmerk van een vrije samenleving waarin noch de overheid, noch de economie geheel de dienst uitmaakt. Daarom zijn er grondrechten, zoals het recht op bescherming van persoonsgegevens, en zijn er in Europees verband grondregels afgesproken om een *level playing field* voor privacygevoelige dienstverlening binnen de Europese Unie te verzekeren.

3 Marktwerking in de sociale zekerheid

In 1998 zijn de ontwikkelingen op het terrein van de sociale zekerheid in een stroomversnelling geraakt. De politieke druk om aan marktwerking te doen is aanzienlijk opgevoerd. In deze stroomversnelling is de bescherming van persoonsgegevens geen rustig bezit. Persoonsgegevens worden steeds vaker 'bedrijfskapitaal'. Institutionele waarborgen komen onder druk te staan. De vraag is hoe de bescherming van persoonsgegevens in de nieuwe context gestalte kan krijgen.

Radicale veranderingen in wetgeving en beleid

'Herijking van verantwoordelijkheden' luidde het nieuwe credo van het eerste paarse kabinet: verantwoordelijkheden moeten daar liggen waar ze het meest doelmatig zijn. Er werd een aantal wetten ingevoerd die werkgevers en werknemers moeten prikkelen om de instroom in de ziekte- en arbeidsongeschiktheidsregelingen te verminderen en de uitstroom te bevorderen. Op 1 maart 1996 trad de Wet uitbreiding loondoorbetalingplicht bij ziekte (WULBZ) in werking. Het resultaat daarvan is dat werkgevers het financiële risico dragen voor het eerste jaar van de ziekte van hun werknemers. Op 1 januari 1998 is het eigen risico voor de werkgevers verder uitgebreid: op die datum trad de wet Pemba (Premiedifferentiatie en marktwerking in arbeidsongeschiktheidsverzekeringen) in werking. De premies worden gerelateerd aan het arbeidsongeschiktheidsrisico van de onderneming. Werkgevers kunnen er ook voor kiezen 'eigen risicodrager' te worden. Dit risico kunnen zij evenals het WULBZ-risico bij een particuliere verzekeringsmaatschappij verzekeren.

Als gevolg van de genoemde beleidswijzigingen is de monopoliepositie van de publieke uitvoeringsorganisatie doorbroken en raken particuliere verzekeringsmaatschappijen dichter betrokken bij de sociale verzekeringen. Voorts heeft de nadruk op preventie van ziekteverzuim en reïntegratie van zieke werknemers geleid tot intensivering van de interactie tussen de sociale zekerheid en de gezondheidszorg. Op ondernemingsniveau is de rol van de arbo-arts in de vormgeving en uitvoering van het arbeidsomstandighedenbeleid alsmede de begeleiding en de reïntegratie van zieke werknemers cruciaal. Het vergroten van de financiële prikkels voor de werkgevers heeft tot gevolg dat werkgevers de prestaties van de arbo-artsen kritisch volgen. De interactie tussen sociale zekerheid en gezondheidszorg komt vooral tot uiting in een aantal ontwikkelingen op de verzekeringsmarkt, in het bijzonder in het aanbieden van geïntegreerde dienstverlening ten behoeve van werkgevers, werknemers en overige burgers: employee benefits.

Wijzigingen in beleid en wetgeving hebben ook plaatsgevonden op het terrein van de werkloosheid. De instrumenten die de arbeidstoeleiding van werkzoekenden beogen te bevorderen zijn aangescherpt. Er zijn wijzigingen doorgevoerd in de Arbeidsvoorzieningswet en de Algemene bijstandswet. Voorts zijn nieuwe regelingen tot stand gebracht, zoals de Wet inschakeling werkzoekenden en de Wet op de reïntegratie arbeidsgehandicapten. Ook reïntegratie van -tijdelijk- arbeidsongeschikte werknemers leidt tot samenwerking en uitwisseling van gegevens tussen diverse betrokkenen: werkgever, arbo-arts, zorgverleners en verzekeringsmaatschappij. De juridische kaders voor deze samenwerking moeten nog worden ontwikkeld.

In aanvulling op de genoemde beleidswijzigingen zijn ook veranderingen aangebracht in de uitvoeringsstructuur van de sociale zekerheid. Samenwerking en marktwerking zijn daarbij kernbegrippen. De samenwerking tussen gemeenten, regionale besturen voor de arbeidsvoorziening en uitvoeringsinstellingen, onder de noemer 'Samenwerking Werk en Inkomen' (SWI) heeft geleid tot de introductie van de Centra voor Werk en Inkomen (CWI). In deze centra (op één locatie) voeren de betrokken partijen, op basis van een samenwerkingsovereenkomst, de noodzakelijke taken uit met betrekking tot bemiddeling en de voorbereiding van het uitkeringstraject. Daarnaast is de aanzet gegeven voor de invoering van concurrentie in de uitvoering van de sociale verzekeringen. Daartoe is een ontvlechtingoperatie ingezet. Per 1 januari 1996 zijn de bedrijfsverenigingen en de uvi's in bestuurlijke, organisatorische en financiële zin los van elkaar komen te staan. Sindsdien is er sprake van een contractuele relatie met de uvi's. Aanvankelijk werden slechts contracten afgesloten met de bestaande uvi's, maar het is van aanvang af de bedoeling geweest op termijn ook anderen tot de markt toe te laten. Een onderdeel van de ontvlechtingoperatie was ook dat de uvi's (in het jargon de A-poten) onderdeel kunnen zijn van een holding, waarin andere werkmaatschappijen (de B-poten) allerlei verwante, private werkzaamheden verrichten. Om te voorkomen dat in deze holdings publieke en private verantwoordelijkheden, gelden en gegevensstromen niet meer uit elkaar zouden kunnen worden gehouden, is een groot aantal voorschriften opgesteld. De regels hebben onder meer betrekking op de bevoegdheid van de uvi's om andere taken uit te voeren: alleen regelingen mogen worden uitgevoerd die betrekking hebben op aanvullingen op wettelijke uitkeringen. Inmiddels is het inzicht gegroeid dat de erkenningscriteria dermate complex zijn dat er waarschijnlijk geen nieuwe uvi's op de markt zullen komen. De beoogde marktwerking zal dan niet van de grond komen.

Op dit moment staan wij aan de vooravond van wat genoemd wordt de grootste reorganisatie in de geschiedenis van de Nederlandse sociale zekerheid. Het kabinet heeft zeer onlangs zijn nieuwe plannen ontvouwd voor de toekomstige uitvoeringsstructuur. Onder de naam SUWI (Structuur Uitvoering Werk en Inkomen) zal een ingrijpende herschikking van taken en verantwoordelijkheden gaan plaatsvinden. Centraal in de nieuwe structuur staan de CWI's, die voor alle werkzoekenden en aanvragers van een uitkering één loket bieden. Vanuit het CWI wordt de betrokkene primair bemiddeld naar werk. Is dit niet mogelijk en krijgt de betrokkene een bijstandsuitkering, dan wordt verwezen naar de gemeente. Voor een WW- of WAO-uitkering komt de aanvrager terecht bij de uvi nieuwe stijl. De uvi's zullen onderling moeten concurreren om opdrachten te verwerven. Om te zorgen dat er daadwerkelijk meer concurrentie gaat ontstaan, moeten er meer uvi's komen. Daartoe zullen de toetredingsdrempels voor de nieuwe uvi's verlaagd worden. De huidige scheiding tussen de A-poten en de B-poten komt te vervallen. Uvi's zullen meer taken mogen uitbesteden en ook private werkzaamheden mogen verrichten.

Bescherming van persoonsgegevens op de helling?

De turbulente ontwikkelingen op het terrein van de sociale zekerheid en het raakvlak met de gezondheidszorg dwingen tot herbezinning op het huidige systeem van bescherming van persoonsgegevens. Het doorvoeren van marktwerking in de sociale zekerheid impliceert dat de persoonsgegevens steeds meer worden toevertrouwd aan partijen die worden uitgenodigd om op het scherpst van de snede te concurreren. Dit klemt te meer omdat persoonsgegevens in de sociale zekerheid het belangrijkste bedrijfskapitaal vormen en een groeiende economische

waarde vertegenwoordigen. Voor de individuele betrokkenen, op hun beurt, staan grote belangen op het spel; het gaat hier tenslotte om basisvoorzieningen. De individuele burger bevindt zich in een kwetsbare positie; hij is niet vrij in zijn keuze om persoonsgegevens al dan niet voor verwerking beschikbaar te stellen. Daar komt bij dat ook ‘gevoelige’, bijvoorbeeld medische persoonsgegevens in het geding kunnen zijn.

De klassieke structuren waarbinnen de bescherming van persoonsgegevens tot nu toe was gewaarborgd, brokkelen af. De scheiding tussen de publieke uitvoering van de wettelijke sociale verzekeringen en de commerciële uitvoering van de private verzekeringen wordt meer en meer diffuus. Daarmee raken de geheimhouding en het gesloten regime zoals gegarandeerd in de Organisatiewet Sociale Verzekeringen 1997 en de Algemene Bijstandswet achterhaald. Ook het medisch beroepsgeheim komt onder druk te staan: de onafhankelijke positie van de arbo-arts kan eenvoudig in de knel komen, wanneer de arbodienst wordt afgerekend op de ‘resultaten’ vertaald in de kosten van het ziekteverzuim. In verschillende opzichten heeft de Registratiekamer hier in 1998 mee te maken gehad.

Persoonsgegevens bedrijfskapitaal

In 1998 heeft de Registratiekamer geadviseerd over de privacyaspecten van de toekomstige organisatie van de sociale zekerheid, toen nog onder de noemer OSV 2001. In dit advies heeft zij onder meer gesteld dat ongeacht de toekomstige structuur van de sociale zekerheid in ieder geval de basisprincipes van gegevensbescherming in acht moeten worden genomen. Gelet op de bijzondere kenmerken van de sociale zekerheid, de positie van de betrokken individuen en de aard van de gegevens (dwangpositie, gedwongen verstrekking van persoonsgegevens, deels ook ‘gevoelige’ gegevens) heeft de Registratiekamer zich op het standpunt gesteld dat niet kan worden volstaan met het algemene normenstelsel van de aanstaande Wet bescherming persoonsgegevens. Binnen de sociale zekerheid is behoefte aan een specifiek wettelijk toetsingskader. In het kabinetstandpunt over de toekomstige Structuur Uitvoering Werk en Inkomen is dit standpunt overgenomen (zie ook 5.3 onder privatisering en verenigbaar gebruik).

Als gevolg van onder andere de ontvlechtingoperatie in de sociale zekerheid ontstaan in toenemende mate vormen van samenwerking tussen van partijen in de sociale zekerheid en commerciële bedrijven, in het bijzonder de bankassurance groepen. Zowel de aanbieders (uvi’s, banken, verzekeringsmaatschappijen, pensioenfondsen, arbo-diensten etc.) als hun diensten en producten zijn in vergaande mate verstrengeld geraakt. Gegeven het feit dat voor alle betrokken aanbieders geldt dat persoonsgegevens bedrijfskapitaal vormen, dringt de vraag zich op of met de onderlinge verwevenheid van aanbieders, diensten en producten ook de bestanden met persoonsgegevens verknoopt zijn geraakt. Hoewel diverse toezichthouders vanuit hun verschillende invalshoeken toezien op het informatiemanagement binnen de financiële conglomeraten, is het bestaande beeld gebrekkig. Iedere toezichthouder ziet slechts een deel van het geheel. Dit roept de vraag op wat er feitelijk gaande is. Het wettelijke uitgangspunt is nu dat gegevens die voor publieke doeleinden ter beschikking zijn gesteld niet mogen worden gebruikt voor commerciële doeleinden. De Algemene Rekenkamer heeft in een rapport dat eind 1998 verscheen geconstateerd dat de scheiding tussen publieke taken en commerciële activiteiten niet voldoende wordt gehandhaafd. De Nederlandse Mededingingsautoriteit (Nma) heeft zich op het standpunt gesteld dat het gebruik van persoonsgegevens voor zowel wettelijke taken als private taken binnen beperkte

randvoorwaarden mogelijk zou moeten zijn. Deze kwestie is actueel nu ABN/Amro en Aegon hebben aangekondigd als nieuwe uvi tot de markt te zullen toetreden, mits de persoonsgegevens die zij voor publieke doeleinden vergaren, ook voor private doeleinden gebruikt mogen worden.

De signalen die de Registratiekamer in 1998 hebben bereikt over het informatiemanagement in financiële conglomeraten en de voorgenomen reorganisatie van de sociale zekerheid, maken dat de Registratiekamer de tijd rijp acht voor een onderzoek. Bij dit onderzoek, dat in 1999 van start zal gaan, zullen ook andere toezichthouders betrokken worden. Doel van het onderzoek is het bevorderen van de inzichtelijkheid van het gegevensmanagement binnen financiële conglomeraten alsmede een inschatting maken van de integriteit van het informatieverwerkend proces en het informatiemanagement (zie ook hoofdstuk 2).

In 1998 werd de Registratiekamer al betrokken bij de ontwikkeling van SWI. De Registratiekamer heeft benadrukt dat uitsluitend gegevens mogen worden verstrekt die partijen nodig hebben voor de uitoefening van hun taken. In de visie van de Registratiekamer is het niet onontkoombaar dat kennisneming van elkaars volledige gegevensset plaatsvindt. De totstandkoming van één SUWI-loket in de toekomst zal niet kunnen leiden tot één database waaruit alle betrokken partijen vrijelijk mogen putten. Onvermijdelijk zal er wel meer dossieroverdracht moeten plaatsvinden. Uitwisseling van gegevens blijkt bijvoorbeeld nu al onvermijdelijk binnen het kader van de samenwerking tussen de publieke en de private arbeidsbemiddeling. Over het zogenaamde samenwerkingsverband ASV (Arbeidsvoorziening Start Vedior) bereikten de Registratiekamer in 1998 diverse klachten van werkzoekenden. De betrokken partijen bleken onder meer op te ruime wijze gebruik te maken van de beschikbaarstelling van informatie. In dit verband heeft de Registratiekamer een aantal concrete aanbevelingen gedaan (Brief van 29 juni 1998 97/0666.2 en 97/0968.11 aan de algemene arbeidsvoorziening). In 1999 verschijnt een rapport over het juridische kader waarbinnen samenwerking en daarmee gepaard gaande uitwisseling van gegevens tussen de deelnemers van SWI en uitzendbureaus in het kader van arbeidstoeleiding kan plaatsvinden.

Medisch beroepsgeheim onder druk

Dat de relatie patiënt-beroepsbeoefenaar in toenemende mate wordt beïnvloed door derde partijen is in 1998 gebleken. De overheid oefent onder meer invloed uit wanneer het gaat om indicatiestelling, in de thuiszorg en de gehandicaptenzorg. Voorts oefenen marktpartijen, zoals Arbo-diensten en verzekeringsmaatschappijen invloed uit. Uit onderzoek van de FNV is gebleken dat het risico dat de opdrachtgever/werkgever, op wie het financiële risico uiteindelijk drukt, zal trachten de arbo-arts te beïnvloeden, reëel is. Gebleken is ook dat de verzekeringsmaatschappij waar het verzuimrisico is verzekerd, op de arbo-arts druk uitoefent om gegevens van de zieke werknemers te verstrekken.

De rol van de particuliere verzekeraars op het raakvlak van de sociale zekerheid en de gezondheidszorg verdient nadere aandacht. Het kabinet heeft in het regeerakkoord van 1998 het standpunt ingenomen dat particuliere verzekeraars op termijn ziekenhuizen mogen beheren. Los daarvan heeft de NMa gesteld dat zorgverzekeraars als ondernemingen moeten worden gezien. Een en ander roept in combinatie met de budgettering van de gezondheidszorg vragen op met het oog op de toegang tot de zorg en het voorkomen van risicoselectie. Voor beide onderwerpen geldt dat persoonsgegevens ten grondslag zullen liggen aan de in dit

verband over individuen te nemen beslissingen. Dit probleem wordt klemmender wanneer in de toekomstige gezondheidszorg nieuwe instrumenten worden toegepast, zoals *managed care*. Bij managed care worden vraag en aanbod in de zorg op elkaar afgestemd met behulp van informatiemanagement door een derde partij, tussen de medische beroepsbeoefenaar en de patiënt in. In 1998 heeft de Registratiekamer een verkennende studie over managed care en de bescherming van persoonsgegevens gepubliceerd. Managed care kan betekenen dat op grote schaal medische gegevens worden uitgewisseld tussen werkgevers, zorgverzekeraars, hulpverleners en de farmaceutische industrie. Met name zorgverzekeraars beschikken over een schatkamer vol gegevens van hun verzekerden.

Nieuwe infrastructuur: RINIS en CVCS

De veranderingen in de sociale zekerheid hangen nauw samen met een intensiever gebruik van technische voorzieningen. De ontwikkeling van RINIS (het RouteringsInstituut voor Nationale InformatieStromen) en het CVCS (het Cliënt Volg Communicatie Stelsel) in de sociale zekerheid zijn daarvan voorbeelden. Het ziet er zelfs naar uit dat de technische ontwikkelingen niet alleen faciliterend worden, maar zelfs bepalend worden voor de organisatorische vormgeving.

Het CVCS biedt de technische infrastructuur om persoonsgegevens uit te wisselen tussen de drie kolommen: uitvoeringsinstellingen, sociale diensten en arbeidsvoorziening. In 1998 heeft de Registratiekamer de Stichting CVCS geadviseerd. De Registratiekamer heeft benadrukt dat het enkele feit dat er tussen de drie kolommen wordt samengewerkt niet rechtvaardigt dat de kolommen onbeperkte toegang krijgen tot elkaars bestanden. Soms kent de techniek echter wezenlijke beperkingen: in het kader van ASV blijkt bijvoorbeeld dat het huidige PGI-systeem het niet mogelijk maakt om gegevens van werkzoekenden selectief af te schermen. Omdat dit in het nieuwe systeem (AGORA) wel mogelijk zal zijn, heeft de Registratiekamer in 1998 te kennen gegeven dat zij het voorshands voldoende acht dat organisatorische maatregelen worden genomen (Brief van 29 juni 1998 97/0666.2 en 97/0968.11 aan de algemene directie van de arbeidsvoorziening).

De belangrijke rol die in de sociale zekerheid is toebedeeld aan de techniek, maakt dat steeds meer partijen aansluiting willen tot de bestaande voorzieningen. Diverse organisaties, bijvoorbeeld uit de hoek van de gezondheidszorg, wensen toegang tot RINIS. De kring van deelnemers aan RINIS is echter beperkt tot de instanties die krachtens de wet bevoegd zijn om het sofi-nummer te gebruiken. Naar het oordeel van de Registratiekamer moet dit uitgangspunt worden gehandhaafd en dient de uitwisseling van gegevens via RINIS beperkt te blijven tot de behartiging van publiekrechtelijke taken.

In de toekomstige uitvoeringsstructuur van de sociale zekerheid wordt de belangrijke rol van de technologische infrastructuur nog eens extra benadrukt. SUWI zal gebouwd worden op CVCS en RINIS, dat dienst zal doen als instrument om de dossieroverdracht tussen de betrokken partijen te realiseren. De globale lijnen van de SUWI-nota tekenen een hybride uitvoeringsstelsel, met een labyrint van gegevensverwerkingen waarbij de ICT een doorslaggevende rol in de bescherming van de privacy krijgt toebedeeld. Het spreekt in de visie van de Registratiekamer voor zich dat niet met technische beveiliging van de gegevensverwerking tegen onrechtmatige toegang van buiten kan worden volstaan. Het gaat er tenslotte om duidelijk af te schermen of persoonsgegevens gebruikt mogen worden, zo ja,

voor welke doeleinden en wie er binnen en buiten de organisatie toegang tot persoonsgegevens mogen krijgen. Ook in dat opzicht kan de techniek, bijvoorbeeld in de vorm van PET, een belangrijke rol vervullen. Technisch gezien is het goed mogelijk om 'chinese muren' op te trekken. Een voorwaarde daarvoor is wel dat de structuur van de uitvoeringsorganisatie helder is, en dat de juridische normen zich in technische oplossingen laten vertalen.

Nieuw kader voor bescherming van persoonsgegevens

De ontwikkelingen volgen elkaar in zeer hoog tempo op en brengen ingrijpende veranderingen teweeg in het stelsel van met name de sociale zekerheid. Partijen proberen hun positie veilig te stellen en verkennen de grenzen van wat juridisch geoorloofd is op het terrein van de bescherming van persoonsgegevens.

Deze ontwikkelingen vergen bijzondere aandacht voor, en investeringen in het handhaven van een adequaat niveau van bescherming van persoonsgegevens. De Registratiekamer ziet zeker mogelijkheden om ook binnen een stelsel van groeiende marktwerking de bescherming van persoonsgegevens in de nieuwe omgeving afdoende te regelen. Het vertrouwen op marktwerking en het vertrouwen in het zelfregulerend vermogen van partijen heeft echter grenzen. Persoonsgegevens vormen immers het bedrijfskapitaal. Hier is een taak voor de overheid weggelegd om de grenzen af te bakenen. Het nieuwe wettelijke toetsingskader zal ontwikkeld moeten worden in directe relatie tot de definitieve besluitvorming over de toekomstige uitvoeringsorganisatie van de sociale zekerheid. De interactie tussen de sociale zekerheid en de gezondheidszorg verdient daarbij specifieke aandacht. Daarnaast zal, in het licht van de verwevenheid van aanbieders, diensten en producten op dit terrein, ook de handhaafbaarheid van de te ontwikkelen normen gewaarborgd moeten worden. De marktwerking zal eerder tot meer regels dan tot minder regels leiden. Illustratief is de regelgeving die in het recente verleden nodig bleek om ongewenste neveneffecten van de ontwikkelingen in de sociale zekerheid te ondervangen en de bescherming van persoonsgegevens te waarborgen. Voorbeelden zijn de medische besluitenregeling in de wet Pemba en de Wet op de medische keuringen. Naast normontwikkeling en een toereikende handhaving van de normen zal in de toekomstige organisatie een zeer belangrijke rol zijn weggelegd voor de techniek in de ontwikkeling van een privacyveilige inrichting van de systemen op het terrein van de sociale zekerheid.

4 Vertrouwelijk communiceren

Na een aarzelende start lijkt de liberalisering van de telecommunicatiemarkt in 1998 op volle snelheid te zijn gekomen. Het aanbod van telecommunicatiebedrijven, netwerken en diensten breidt zich snel uit. Voor de gebruikers -zowel zakelijk als privé- ontstaan steeds meer keuzemogelijkheden. Wie bereikbaar wil zijn beschikt niet slechts over enkele gewone telefoonnummers (met voicemail) en faxnummers maar ook over een mobiel nummer en een e-mailadres, in de verwachting dat anderen ook daarmee zijn uitgerust. Communicatiemiddelen sluiten beter aan op afzonderlijke gebruikers, ze zijn goedkoper dan ooit en dienen het gemak. Daarom is het paradoxaal dat de mogelijkheden tot het vertrouwelijk communiceren geen gelijke tred hebben gehouden. Integendeel. In toenemende mate moeten gebruikers er rekening mee houden dat ook anderen dan de door henzelf gekozen communicatiepartners kennis kunnen nemen van berichten. Daarnaast bestaat er een levendige belangstelling voor gegevens over het communicatieverkeer. In 1998 is vertrouwelijke communicatie opnieuw onderwerp geweest van maatschappelijk debat.

Ontwikkelingen in de telecommunicatiemarkt

Het nieuwe telecommunicatielandschap wordt gekarakteriseerd door een aantal ontwikkelingen. Dominant is de vrijwel volledige liberalisering van de telecommunicatiemarkt, waardoor het aantal aanbieders van infrastructuren, netwerken en diensten zeer sterk is gestegen. Waar een aantal jaren geleden telefonie bijvoorbeeld nog een staatsmonopolie was, waren er aan het eind van 1998 honderden aanbieders van telefoniediensten.

Technische ontwikkelingen in de telecommunicatie vinden steeds sterker hun weerslag in het maatschappelijk verkeer. E-mail begint een grotere rol te spelen, voor zowel persoonlijke als zakelijke communicatie. De investeringen van veel bedrijven, bijvoorbeeld de banken, in het inrichten van hun dienstverlening via het Internet geven ook een duidelijk signaal. Naar verwachting zal binnen een aantal jaren een aanzienlijk deel van de zakelijke transacties via dit medium worden uitgevoerd. Nu deze nieuwe media de rol van de traditionele post en telefonie gaan overnemen, ontstaan ook zorgen over de bescherming van de inhoud van de communicatie. Kan een gebruiker van deze nieuwe diensten en nieuwe infrastructuren, die ook nog eens door nieuwe, minder bekende marktpartijen worden aangeboden, er nog wel van uitgaan dat er zorgvuldig met zijn communicatie-uitingen wordt omgegaan? De nieuwe technologieën leiden immers tot de nodige vragen over beheer en beveiliging van de communicatie. Op het Internet bijvoorbeeld is van een nauwgezette netwerkbeveiliging nauwelijks sprake: de gegevens worden in pakketten over publieke netwerken gerouteerd, via een niet van tevoren bekende weg en passeren daar bij netwerken en knooppunten die onder beheer van derde partijen staan. Ook het gemak waarmee e-mailverkeer, bijvoorbeeld bij Internet service providers, kan worden gekopieerd baart zorgen. Doordat netwerktechnologie bovendien de grenzen van ruimte en tijd beïnvloedt, denk aan telewerken, wordt bijvoorbeeld ook de scheiding tussen zakelijke en persoonlijke communicatie minder helder.

Een belangrijke ontwikkeling is ook de convergentie: de traditionele koppeling van bepaalde diensten aan een daarvoor speciaal ontwikkeld netwerk is komen te vervallen. Hier zijn tal van voorbeelden bij te bedenken. Een fax kan worden verstuurd vanaf de computer,

telefoneren kan ook over het Internet en de post komt niet alleen meer door de gleuf van de deur maar druppelt ook binnen in de *mailbox* via de kabelaansluiting. Door de convergentie zijn de scheidslijnen tussen openbare en publieke omgevingen onduidelijker geworden en doen zich nieuwe beveiligingsvraagstukken voor. Kabelnetwerken, bijvoorbeeld, zijn *shared medium* netwerken die oorspronkelijk niet gebouwd zijn voor vertrouwelijke communicatie: de informatie op dergelijke netwerken wordt in principe bij alle aangeslotenen afgeleverd. Voor het gebruik van kabelnetwerken voor telefonie dienen dan ook zodanige beveiligingsmaatregelen te worden getroffen dat niet iedereen ook kennis kan nemen van dergelijke vertrouwelijke informatie.

De belangstelling voor de gegevens over de gebruikers is toegenomen. Het kennen van het communicatiegedrag is steeds belangrijker geworden voor het werven en binden van klanten of juist voor het afwijzen van sommige potentiële klanten. Abonnementsvormen op basis van het belgedrag zijn daarvan een voorbeeld. Voorkomen dat klanten overstappen naar de concurrent is met name in de mobiele markt zeer belangrijk omdat de kosten van het werven van klanten veelal pas worden teruggewonnen als de klant voldoende lang zijn abonnement houdt. Het systematisch bijhouden van grote hoeveelheden klantgegevens en de analyse daarvan met behulp van *datamining*, zijn in de telecombranche sterk in opkomst. Ook bij het beperken van risico's door het signaleren van potentiële wanbetalers en het opsporen en voorspellen van fraude wordt gebruik gemaakt van deze gegevens. Deze ontwikkelingen benadrukken dat niet alleen bescherming van de inhoud van de communicatie van belang is, maar dat ook verkeersgegevens, de gegevens over het telecommunicatieverkeer aandacht behoeven.

Wetgeving als oplossing?

In het parlement ontbrandde een heftige discussie over de bescherming van nieuwe communicatievormen. Het wetsvoorstel tot herziening van artikel 13 van de Grondwet ondervond veel tegenstand in en buiten het parlement. Daarvoor had de minister van Justitie het publieke debat al geopend met de uitspraak dat aan E-mail berichten dezelfde bescherming toekomt als aan open briefkaarten: geen. Daarop viel het nodige op af te dingen. Immers, wie een ansicht in de brievenbus post kan niet klagen dat de posterijen kennis nemen van het bericht. Wel terecht is het vertrouwen dat de posterijen geen gebruik maken van die kennis of die aan derden verder verstrekken. Doen zij dat toch dan maken zij zich schuldig aan een strafbaar feit. Dat in de optiek van de minister de verzender van een e-mail bericht zich nog minder illusies hoefde te maken over de vertrouwelijkheid daarvan dan de afzender van een ansichtkaart, stemde niet positief. In de toelichting bij het wijzigingsvoorstel werd de indruk gewekt dat alleen vertrouwelijke vormen van telecommunicatie nog bescherming zouden genieten. De vertrouwelijkheid zou –net als bij de open briefkaarten- worden afgemeten aan de mate van beveiliging die de zender zou gebruiken. Niet-versleutelde e-mail zou derhalve door wie dan ook kunnen worden gelezen. Of niet-versleutelde telefoongesprekken voortaan hetzelfde lot zou zijn beschoren bleef nog enigszins onduidelijk. Later haastte de regering zich te bevestigen dat uiteraard alle vertrouwelijke communicatie grondwettelijke bescherming zou krijgen. Toch roept de beoogde bescherming van e-mailverkeer nog steeds de nodige vragen op. Mogen beheerders van lokale en private netwerken straffeloos e-mailberichten die in hun systemen zijn opgeslagen maar die niet voor hen zijn bestemd, inzien en bekendmaken? Het zou beter zijn om daarover zekerheid te bieden in de tekst van de grondwet dan in verschillende, soms tegenstrijdige toelichtingen op dit punt.

Voor wat betreft de bescherming van gegevens over het communicatieproces, verkeersgegevens, moet worden geconstateerd dat het niet altijd eenvoudig is een duidelijke lijn te ontdekken in het politieke debat. Stelde de regering in het voorstel tot wijziging van artikel 13 GW voor de verkeersgegevens geen grondwettelijke bescherming te verlenen, bij amendement aanvaardde de Tweede Kamer een wijzigingsvoorstel dat wel bescherming biedt. Voor de regering maakte het kennelijk geen wezenlijk verschil of verkeersgegevens voortaan onder de bescherming van artikel 13 GW vallen of niet. Het geamendeerde wetsvoorstel werd vervolgens bij de Eerste Kamer ingediend. Bij de behandeling in de Eerste Kamer keerden partijen die in de Tweede Kamer het initiatief tot de betreffende amendering hadden genomen weer op hun schreden terug. Bij nader inzien zou met verkeersgegevens niets bijzonders aan de hand zijn. Ze zouden hetzelfde kunnen worden behandeld als andere gevoelige gegevens (zoals ras of seksuele geaardheid) die bescherming genieten in de algemene privacywetgeving op basis van artikel 10 GW.

Bij de vrijheid om met anderen te communiceren hoort echter dat niet alleen de inhoud van de communicatie maar ook de informatie over het communicatieverkeer vertrouwelijk blijft. Dit belang is van een andere orde dan het belang niet te worden gediscrimineerd op basis van een gevoelig gegeven. In afwachting van de uitkomsten van de thans ingestelde Commissie grondrechten in het digitale tijdperk is het wijzigingsvoorstel voor artikel 13 GW aangehouden.

Overheidscontrole

Er zijn aanwijzingen dat de overheid probeert op nieuwe vormen van communicatietechnologie maximale greep te krijgen. Hiermee komen waarden in de knel als de vrijheid van meningsuiting en het recht op privacy. Kennelijk zijn de grondrechten in de on-line wereld geen vanzelfsprekende zaak. De regeringsnota Wetgeving voor de elektronische snelweg (TK 1997-1998, 25 880, nrs. 1-2) bevatte een goede aanzet voor normvorming, ook voor de bescherming van de privacy. Tegelijkertijd zette de regering echter ontwikkelingen in gang die niet spoorden met de uitgangspunten van de nota. Zo omarmde de regering het PET-concept, het inzetten van technologie om privacy te beschermen en sloeg daarmee het pad naar anonimiteit in. Maar daar tekende ze bij aan dat burgers moeten accepteren dat hun identiteit altijd bij een van de actoren op de digitale snelweg bekend zal zijn. Van vele kanten is aangedrongen op bijstelling van het ambitieniveau van de opsporingsinstanties op de digitale snelweg. Ook tijdens de jaarvergadering van de Nederlandse Juristenvereniging die was gewijd aan Internet is hiervoor uitdrukkelijk aandacht gevraagd.

Bij alle commotie rond artikel 13 GW is het velen ontgaan dat in de nieuwe Telecommunicatiewet geen verplichting meer is opgenomen tot naleving van het communicatiegeheim. Naar de opvatting van de Registratiekamer beperkt het communicatiegeheim zich niet tot de inhoud van het gegevensverkeer en strekt het zich uit tot de verkeersgegevens. De bescherming die de Telecommunicatiewet biedt richt zich te eenzijdig op de bescherming van de persoonlijke levenssfeer en heeft onvoldoende aandacht voor de bescherming van zakelijke communicatieprocessen. Een aardig gedachte-experiment biedt bijvoorbeeld ook het loggen door Internet service providers (ISP) van de interactie van een gebruiker met een website. Strikt genomen is dat een communicatievorm waar derden

zoals ISP's niets mee te maken hebben. Er gaan nog nauwelijks geluiden op om de grondwettelijke bescherming ook daartoe uit te breiden, hoewel dat wel voor de hand ligt
.
In artikel 13.4 Telecommunicatiewet is een gevaarlijk precedent geschapen door de telecommunicatiesector te verplichten over alle verkeer gegevens te vergaren en beschikbaar te houden buiten de eigen bedrijfsvoering om. Ook van onverdachte personen worden dus de gegevens klaar gezet voor mogelijke raadpleging door de autoriteiten. Wanneer daarbij ook de herziening van artikel 125f van het Wetboek van Strafvordering (WSv) wordt betrokken, die de bevoegdheid tot het vorderen van inlichtingen over het telecommunicatieverkeer van niet-verdachte personen betreft, dan ontstaat een situatie met vergaande controlebevoegdheden van het telecomverkeer. Daarnaast was beoogd dat ook private netwerken bij ministeriele beschikking verplicht konden worden te voldoen aan de eisen van aftapbaarheid (artikel 13.7 Telecommunicatiewet). Hiervan is door de staatssecretaris van Verkeer en Waterstaat gedurende de behandeling in de Eerste Kamer toegezegd dat van deze mogelijkheid geen gebruik zal worden gemaakt.

Bijzonder in dit verband is de grondslag voor het aftappen van communicatie over Internet. De regering houdt eraan vast dat stromende gegevens, die zich in een toestand van telecommunicatie bevinden moeten worden afgetapt op basis van 125g WSv. Onderscheidend criterium is in de visie van het kabinet of een gegeven valt te raadplegen op een door de mens te bepalen tijdstip. In die visie moet een telecommunicatienetwerk kennelijk worden beschouwd als een black box. Daarbij moet als juridische fictie worden aangenomen, dat de gegevens ook als ze tijdens het transport worden opgeslagen als stromend moeten worden beschouwd. De grens is hier niet helemaal duidelijk In de praktijk blijken vorderingen uit te gaan van het openbaar ministerie waarbij ISP's worden gesommeerd elke vijf minuten de database te raadplegen. Dat is geen tappen van stromende gegevens. Het is de vraag of het onderscheid tussen computerhuiszoeking en het tappen van telecommunicatie-netwerken nog wel zinvol is. Het zou beter zijn dat een stelsel van waarborgen in het leven wordt geroepen dat zich richt op het gehele proces van verwerking van informatie, ongeacht de fase of de plaats waar een bericht zich bevindt. Een dergelijke benadering doet meer recht aan de huidige stand van de ICT. Ook in dit opzicht valt het toe te juichen dat de Commissie grondrechten in het digitale tijdperk zich nader in deze problematiek zal verdiepen.

De hoofdlijnen voor de strafrechtelijke aansprakelijkheid van tussenpersonen zoals neergelegd in het -aangepaste- wetsvoorstel Computercriminaliteit II zijn op zich aanvaardbaar. Van de ISP wordt niet verwacht dat hij alle uitingen op Internet controleert of bijhoudt. Hoe een en ander in de praktijk zal uitwerken is wel een bron van zorg. Inmiddels lijkt de gelijkstelling van de ISP met een uitgever door de Nederlandse wetgever in conflict te komen met het voorstel van de Europese Commissie in de ontwerp richtlijn voor E-commerce. Daarin wordt een meer genuanceerde regeling gevolgd.

Anonimiteit

Iedere burger moet er voor kunnen kiezen anoniem te blijven bij het verkrijgen van toegang tot Internet. Ook mogelijkheden om anoniem te betalen zijn essentieel voor de elektronische snelwegen, als men daar dezelfde bescherming van privacy wil genieten als in het dagelijks

leven. Het streven van de Nederlandse overheid naar het uitsluitend toestaan van geïdentificeerd en dus controleerbaar gebruik van openbare telecommunicatiemiddelen staat op gespannen voet met het geldende recht. De Recommendation 3/97 ‘Anonimity on the Internet’ van de Working Party on the Protection of Individuals with regard to the Processing of Personal Data dringt er op aan dat lidstaten er in hun wetgeving voor zorgen dat het gebruik van Internet mogelijk wordt gemaakt met een minimaal gebruik en minimale verspreiding van persoonsgegevens.

Vooruitbetaalde telefoonkaarten (prepaid cards) voor mobiele telefoons zouden alleen mogen worden verkocht aan klanten die zich zouden laten registeren. Dit was een voornemen van het kabinet, waartegen ondermeer door de Registratiekamer met kracht is geopponeerd. De verkooppunten zouden de gegevens vervolgens beschikbaar moeten houden voor politie en inlichtingendiensten. Deze gedachte werd ingegeven door de angst dat criminelen hun telefonische activiteiten aan de waarnemingen door de politie zouden kunnen onttrekken. Vanuit opsporingsinstanties wordt dan ook stevig aangedrongen op het onmogelijk maken van anoniem telecommunicatieverkeer. De prepaid beller zou daarmee op een lijn worden gezet met een kleine minderheid van wetsovertreders. Maar telefoneren is in de regel niet ‘gevaarzettend’. Het dragen van een kenteken is -hoe dwingend deze metafoor ook lijkt- niet nodig op de elektronische snelweg. De digitale snelweg is geen openbare ruimte zoals de (fysieke) openbare weg. Van het eerder bedoelde voornemen heeft het kabinet -in elk geval voorals nog- afgezien.

Cryptografie en TTP’s

Voor de gebruiker is het steeds minder inzichtelijk of de beveiliging van netwerken en infrastructuren nog voldoet aan hetgeen hij op grond van zijn recht op vertrouwelijke communicatie mag verwachten. Dit geldt te meer voor de in opmars zijnde draadloze communicatie, die door een bezitter van een geschikte antenne-installatie opgevangen kan worden. Het gebruik van open netwerken leidt er in de praktijk toe dat in toenemende mate eindgebruikers zelf gaan zorgen voor de beveiliging van hun communicatie. Dit betreft zowel persoonlijke communicatie, als zakelijke communicatie waar partijen hun bedrijfsgeheimen willen afschermen voor derden. Cryptografie, het versleutelen van berichten, is een geëigend middel hiervoor. Naast het garanderen van de vertrouwelijkheid van de informatie, kan cryptografie ook bijdragen aan de andere basisvoorwaarden voor beveiliging van gegevens, authenticiteit en integriteit. Asymmetrische systemen bieden, onder voorwaarden, de mogelijkheid om de verzender van een bericht te authenticeren aan de hand van een digitale handtekening. Bij sommige methoden kan met deze handtekening ook de integriteit van de communicatie worden getoetst, bijvoorbeeld door het gebruik van hash-functies die controlegetallen genereren: bij wijziging van de inhoud van het bericht wijzigt in zo’n geval ook de handtekening. De ontvanger kan dus nagaan of er door derden met het bericht geknoeid is.

Bij de introductie op grote schaal van cryptografie doet zich een aantal knelpunten voor. Naarmate de cryptografische technieken waarover burgers en bedrijven beschikken krachtiger worden, vooral door het gebruik van langere sleutels, wordt het afluisteren daarvan door instanties belast met de opsporing van strafbare feiten of de nationale veiligheid steeds moeilijker. Opsporingsinstanties hebben dan ook belang bij het wettelijk voorschrijven van de maximale sleutellengte die is toegestaan voor gebruik in het maatschappelijk verkeer, of het

verplichten van het bewaren van de cryptografische sleutels. De Registratiekamer is echter van mening dat het niet wenselijk is dat het gebruik van zware cryptografie wordt voorbehouden aan een beperkt aantal overheidsdiensten. Bij andere vormen van de inzet van zware cryptografie moet zowel worden gedacht aan de bescherming van bedrijfsinformatie als aan de bescherming van gevoelige persoonsgegevens. De oplossing van deze problematiek moet derhalve gezocht worden binnen het spanningsveld van privacy enerzijds en opsporing van strafbare feiten en nationale veiligheid anderzijds. Trusted Third Parties (TTP's) vormen een belangrijke schakel bij het inrichten van betrouwbare cryptografische systemen voor publiek gebruik. De Registratiekamer heeft aangedrongen op het toelaten van meerdere TTP's met een concurrerend belang en op een scheiding tussen TTP-diensten voor authenticiteit en integriteit en TTP-diensten voor vertrouwelijkheid. De aankondiging door de minister van Binnenlandse Zaken van 18 februari 1998 van een deponeringsplicht van sleutels bij de overheid was daarmee in tegenspraak (Kamerstukken II, 1997-1998, 21 501-10, nr. 38).

De stormachtige groei van communicatiemiddelen houdt geen gelijke tred met de mogelijkheden om vertrouwelijk met anderen te communiceren. De zorg van de overheid om in voorkomende gevallen de inhoud van het gegevensverkeer, maar tegenwoordig vooral ook gegevens over communicatieprocessen, te kunnen controleren versterkt deze ontwikkeling. De Registratiekamer acht het onontkoombaar dat ook in technische zin oplossingen worden ontwikkeld waarmee tegemoet wordt gekomen aan de maatschappelijke behoefte om vertrouwelijk te communiceren. Daarbij moet niet alleen worden gedacht aan cryptografie, maar ook aan de inzet van *privacy enhancing technologies*, technische beschermingsmaatregelen in het ontwerp van systemen, om de verkeersgegevens te beschermen.

5 Activiteiten van de Registratiekamer

5. 1 Communicatie

Investeren in voorlichting en in de communicatie met de verschillende doelgroepen is een belangrijk spoor waarlangs de Registratiekamer de bescherming van de privacy en het zorgvuldig gebruik van persoonsgegevens structureel bevordert. De Registratiekamer organiseerde in het verslagjaar verschillende bijeenkomsten om overleg te voeren met de betrokken en belanghebbende partijen. Zo werden in januari 1998, in samenwerking met het ministerie van Binnenlandse Zaken, een drietal proefprocessen en een discussiebijeenkomst gehouden met vertegenwoordigers van de overheid, rechterlijke macht, politie en bedrijfsleven over het wetsvoorstel Bevordering integere besluitvorming openbaar bestuur (BIBOB). In februari werd een workshop georganiseerd over de informatiegaring door de fiscus en in mei een over cliëntvolgsystemen. In de herfst organiseerde de Registratiekamer een conferentie over privacybescherming en *managed care*, met vertegenwoordigers van zorgverzekeraars en belangenorganisaties op het gebied van de gezondheidszorg. In november organiseerde de Registratiekamer een workshop naar aanleiding van een discussienota over de gegevensuitwisseling tussen (partners van) Centra voor Werk en Inkomen (CWI's) en uitzendbureaus. De discussies hebben hun weerslag gevonden in publicaties (zie bijlage 4).

Daarnaast leverde de Registratiekamer in 1998 bijdragen aan congressen en studiebijeenkomsten over onder meer personeelsvolgsystemen, direct marketing, sociale zekerheid, camerabewaking en elektronische dossiers in de gezondheidszorg. De Registratiekamer heeft ook meegewerkt aan diverse congressen en studiebijeenkomsten over de nieuwe Wet bescherming persoonsgegevens.

Om te bevorderen dat privacybescherming ook op de politieke agenda haar plaats behoudt, richtte de Registratiekamer zich met regelmaat tot regering en parlement. Ten tijde van de kabinetsformatie wees de Registratiekamer er in een brief aan de informateurs op dat in de privatisering van de sociale zekerheid, de liberalisering van telecommunicatie en de beleidsontwikkeling in de gezondheidszorg de bescherming van de privacy van de burger een prominente plaats moet krijgen. Tijdens de behandeling van de Telecommunicatiewet in de Tweede en in de Eerste Kamer heeft de Registratiekamer, in vervolg op de adviezen die ze daarover heeft uitgebracht, deelgenomen aan hoorzittingen (zie hoofdstuk 4). Ook nam de Registratiekamer deel aan een hoorzitting in de Tweede Kamer over het wetsontwerp 'Rekening rijden'.

In 1998 hebben medewerkers van de Registratiekamer regelmatig gastcollege's verzorgd bij universiteiten en andere onderwijsinstellingen. Het is opmerkelijk dat het onderwerp privacy en de bescherming van persoonsgegevens in steeds meer opleidingen op HBO en universitair niveau een vast onderdeel is geworden.

De mediavoorlichting, tenslotte, is ook 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. Naast de interviews en medewerking aan radio- en televisieprogramma's, publiceerde medewerkers van de Registratiekamer artikelen in verschillende vakbladen (zie bijlage 5). In het tweemaandelijks tijdschrift *Privacy & Informatie* -waarvan begin 1998 het eerste nummer

verscheen- verzorgt de Registratiekamer een katern waarin samenvattingen zijn opgenomen van de belangrijkste uitspraken, adviezen aan de regering en publicaties.

[*Privacy & Informatie*, Sdu Uitgevers]

Van het telefonisch spreekuur is in het verslagjaar veelvuldig gebruik gemaakt. Circa 5500 burgers, bedrijven en instanties vroegen om informatie en advies, meestal naar aanleiding van specifieke problemen of klachten. In de meeste gevallen konden die vragen ook telefonisch worden afgedaan.

Door de beperkte capaciteit kan de Registratiekamer ook slechts in beperkte mate een loketfunctie vervullen. Beleid van de Registratiekamer is om zoveel mogelijk te fungeren als 2e lijnsvoorziening door ondersteuning te bieden aan organisaties en instanties die rechtstreeks consumenten, werknemers, patiënten, individuele bedrijven en beroepsbeoefenaars bedienen. In 1998 is daarom veel energie besteed aan het onderhouden van contacten en het ontwikkelen van voorlichtingsmateriaal voor consumentenorganisaties, patiëntenplatforms, vakbonden, maar ook Kamers van Koophandels en branche- en beroepsorganisaties. In 1998 werden 595 schriftelijke verzoeken om advies en voorlichting behandeld. Die verzoeken waren afkomstig van individuele organisaties en bedrijven, maar ook van branche- en beroepsverenigingen en adviesinstellingen. In de bundel *Persoonsgegevens Beschermd* -waarvan in mei 1999 de nieuwe editie verschijnt- publiceert de Registratiekamer een selectie van de uitspraken en adviezen waarin de algemene begrippen, normen en regels van de Wet persoonsregistraties in specifieke situaties zijn toegepast. De samenvatting die van elke uitspraak wordt gegeven, kan als richtsnoer dienen voor de invulling van de normen in vergelijkbare situaties.

Met de ontwikkeling van een eigen website op het Internet (www.registratiekamer.nl) hoopt de Registratiekamer in de toekomst de verschillende doelgroepen nog beter te bedienen. De site bevat onder meer informatie over publicaties, uitspraken en actuele ontwikkelingen en ook antwoorden op veel gestelde vragen.

[www.registratiekamer.nl]

5.2 Ontwikkeling van normen

De belangrijkste juridische basis voor de bescherming van persoonsgegevens is de Wet persoonsregistraties (WPR). In de adviezen die de Registratiekamer in 1998 heeft uitgebracht aan de regering, de klachten en schriftelijke verzoeken om voorlichting en advies die werden behandeld en de onderzoeken die de Registratiekamer heeft ingesteld, zijn een aantal begrippen en normen van die wet nader ingevuld en toegepast in specifieke contexten. Een overzicht van de interpretatie en toepassing van de begrippen en normen van de WPR, is samengebracht in de herziene uitgave van *Persoonsgegevens beschermd*. In het verslagjaar is in het bijzonder aandacht besteed aan transparantie en verenigbaar gebruik.

[Eck, B.M.A. van, e.a., *Persoonsgegevens beschermd. Uitspraken van de Registratiekamer. Gewijzigde uitgave, met verwijzingen naar Wet bescherming persoonsgegevens*. Sdu Uitgevers, Den Haag 1999]

Transparantie

Een belangrijk aspect bij de bescherming van persoonsgegevens is openheid over de gegevensverwerking (transparantiebeginsel). Zo moet de houder de geregistreerden op de hoogte brengen van het feit dat er gegevens zijn opgenomen in de persoonsregistratie (artikel 28 WPR). Ook de aanmelding van de persoonsregistratie bij de Registratiekamer vormt een onderdeel van transparantie bij verwerking van persoonsgegevens (19 en 24 WPR). De transparantie is onder invloed van de desbetreffende Europese richtlijn aangescherpt in de Wet bescherming persoonsgegevens (WBP).

Binnen vier weken nadat de gegevens zijn opgenomen, moet medegedeeld worden aan de geregistreerde dat de persoonsgegevens zijn opgenomen. De mededeling moet met name ook het doel of de doelen van de registratie vermelden. De informatie schoot tekort bij de introductie van de Albert Heijn Bonuskaart. Op het inschrijfformulier voor deze klantenkaart werd niet vermeld wat de bedoeling was van het vastleggen en gebruik van persoonlijke gegevens van de kaartaanvrager. Het bleek te gaan om het analyseren van aankoopgegevens om de klant persoonlijke aanbiedingen te kunnen doen. De aspirant-kaarthouder werd hierover evenmin op enige andere wijze geïnformeerd, zo concludeerde de Registratiekamer. Een belangrijke uitzondering op deze informatieverplichting, dat de geregistreerde redelijkerwijs kon weten dat een dergelijke opname van zijn gegevens voor het beoogde doel heeft plaatsgevonden, achtte de Registratiekamer niet van toepassing. Bij deze uitzondering gaat het namelijk om de informatie die voorafgaand aan de verplichting tot informatieverstrekking redelijkerwijs bekend geacht kon worden. Hiervan was in casu geen sprake (97.V.0034.1).

[De Albert Heijn Bonuskaart werd in januari 1998 met veel publiciteit geïntroduceerd. Op vertoon van de kaart krijgt de klant korting op een aantal producten. Voor elke klant geldt dezelfde korting op dezelfde producten, de kortingskaart is niet persoongebonden. Het is dus niet noodzakelijk dat de klant zijn naam, adres en andere gegevens verstrekt. Albert Heijn wees de klant niet op de optie om de kaart aan te vragen zonder naam, adres, etc. te verstrekken. Albert Heijn maakte aan de klant die zijn gegevens op het aanvraagformulier invulde ook niet duidelijk waar die gegevens voor gebruikt worden. Het oordeel van de Registratiekamer leidde er toe dat Albert Heijn in advertenties en op de formulieren alsnog die duidelijkheid verschafte.]

In de zaak van de Persoonsgebonden Club Card (PCC) was sprake van een verplichte registratie van persoonsgegevens. Dit brengt mee dat naar het oordeel van de Registratiekamer hoge eisen gesteld moeten worden aan de waarborgen ter bescherming van de persoonlijke levenssfeer van de PCC-houder. Zo zal iedere kaarthouder uitdrukkelijk op de hoogte gesteld moeten worden van het doel en gebruik van zijn gegevens, waarbij hem uitdrukkelijk de mogelijkheid moet worden geboden om tegen met name commercieel gebruik van zijn gegevens bezwaar te maken (98.0081.46).

Bij de wijzigingen van het Air Miles spaarsysteem waarbij Loyalty Management Netherlands de aankoopgegevens op productgroepniveau (‘afdelingsniveau’) registreert, oordeelde de Registratiekamer dat hierover voldoende informatie werd verschaft aan bestaande en nieuwe kaartaanvragers. Alle kaarthouders ontvingen bij het kwartaaloverzicht van de gespaarde Miles een folder waarin de voorgestane wijzigingen uit de doeken werden gedaan. Ook werden ze hierbij nog eens uitdrukkelijk in de gelegenheid gesteld om bezwaar te maken tegen het gebruik van hun gegevens voor het toezenden van persoonlijke aanbiedingen.

Transparantie speelt ook een belangrijke rol bij de gegevensuitwisseling tussen verschillende organisaties in de sociale zekerheid via het Routerings Instituut (Inter-)Nationale Informatie Stromen-concept (RINIS). In een advies aan de staatssecretaris van Binnenlandse Zaken heeft de Registratiekamer over de privacyaspecten hiervan geadviseerd. Zij is van oordeel dat gegevensuitwisseling tussen uitvoeringsinstellingen in verschillende sectoren door het RINIS-concept meer beheersbaar, zichtbaar en controleerbaar wordt. Aangezien de deelnemers onderling structureel persoonsgegevens uitwisselen zal het nodig zijn dat aan de geregistreerden nadere informatie wordt verstrekt als dat nodig is om tegenover betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen, gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt. In het kader van RINIS zal deze situatie zich regelmatig kunnen voordoen. Dit geldt niet als goede voorlichting vooraf ertoe heeft geleid dat de betrokkene reeds op de hoogte is (96.A.712) .

Verenigbaar gebruik

Artikel 6, eerste lid WPR schrijft voor dat het gebruik van de persoonsgegevens binnen de organisatie van de houder van de registratie, verenigbaar dient te zijn met het doel van de registratie. Het uitgangspunt van doelgebonden gebruik van persoonsgegevens wordt hierin verwoord voor het gebruik binnen een organisatie. De inwerkingtreding van de thans aanhangige Wet bescherming persoonsgegevens zal het belang van dit begrip nog doen toenemen. Het begrip ‘verenigbaar’ is immers in het ontwerp het sleutelbegrip voor wat betreft de verdere verwerking van persoonsgegevens voor andere doeleinden dan waarvoor ze zijn verzameld. Aan de Registratiekamer wordt regelmatig de vraag voorgelegd of persoonsgegevens, eenmaal vastgelegd in een bepaalde relatie tussen houder en geregistreerde, kunnen worden gebruikt om de geregistreerde ook andere producten, diensten of regelingen onder de aandacht te brengen, eventueel na het maken van bepaalde selecties.

Persoonsgegevens hebben vaak een commerciële waarde. Dat geldt ook voor die persoonsgegevens die worden gebruikt voor communicatiedoeleinden, zoals naam, adres en woonplaats, en telefoonnummer. Het bedrijf dat, of de instelling die dergelijke persoonsgegevens heeft verkregen in verband met de uitvoering van een overeenkomst, als onderdeel van de uitoefening van een publieke taak, of met het oog op het toezenden van bepaalde informatie, zal die gegevens zo leert de ervaring, ook voor andere doeleinden willen gebruiken: bijvoorbeeld om informatie toe te sturen over andere producten, van hetzelfde bedrijf of van een andere maatschappij binnen hetzelfde concern. Ook in het afgelopen jaar is aan de Registratiekamer vanuit verschillende maatschappelijke sectoren de vraag voorgelegd of een dergelijk nevengebruik van gegevens geoorloofd kan zijn, en zo ja, onder welke voorwaarden. De vragen die in dit kader werden voorgelegd betroffen onder meer een mailing waarbij degenen die bij een ziektekostenverzekeraar een verzekering in aanvulling op de ziekenfondsverzekering hadden afgesloten geattendeerd werden op een ander verzekeringsproduct van het concern (97.V.906), en een mailing aan bij een pensioenfonds aangesloten werknemers over aanvullende mogelijkheden, zoals een koopsompolis, bij een andere maatschappij binnen het concern (97.V.782). De vraag of sprake is van verenigbaar gebruik is van groeiend belang omdat dit ook een centrale vraag is bij elke verwerking van persoonsgegevens onder de toekomstige Wet bescherming persoonsgegevens.

[Bij de invulling van het begrip ‘verenigbaar gebruik’ betrekt de Registratiekamer de volgende criteria: (i) de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen; (ii) de aard van de betreffende gegevens; (iii) de gevolgen van de beoogde verwerking voor de betrokkene; (iv) de wijze waarop de gegevens zijn verkregen; (v) de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen. Deze criteria zijn deels gebaseerd op de Europese Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en zijn ook onderdeel van de parlementaire behandeling van de WBP.]

Relevante factoren voor de vraag of persoonsgegevens kunnen worden gebruikt voor de mailings die hiervoor werden genoemd zijn bijvoorbeeld of het gaat om het aanbieden van een verwant product, of de gegevens door de geregistreerde vrijwillig of verplicht zijn verstrekt, of naast de voor communicatie benodigde gegevens nog andere persoonsgegevens zijn gebruikt, en of het daarbij gaat om gegevens die als ’gevoelig’ moeten worden betiteld of die in het algemeen als vertrouwelijk worden beschouwd. Verder is van belang dat het aanbieden van andere producten en diensten binnen een concern aan cliënten geen ongebruikelijke gang van zaken is. Factoren als deze komen ook aan de orde in de Gedragscode Verwerking persoonsgegevens verzekeringsbedrijf (Stcrt. 1998, 44). Daarin wordt een op de verzekeringsbranche toegespitste uitwerking van het begrip ‘verenigbaar’ gegeven. Aan de hand van die factoren wordt duidelijk dat een mailing waarvoor gebruik wordt gemaakt van vrijwillig verstrekte naam-, adres-, en woonplaatsgegevens zonder verdere selectiekenmerken, waarmee binnen hetzelfde concern een verwant product onder de aandacht van verzekerden wordt gebracht, in het algemeen wel als ‘verenigbaar’ gebruik van die persoonsgegevens te beschouwen is, als de geregistreerden niet uitdrukkelijk te kennen hebben gegeven daarop geen prijs te stellen. Als het aanvullingsfonds en het pensioenfonds binnen die grenzen een mailing verzorgen ten behoeve van een andere maatschappij binnen het concern, zal dit gebruik van hun gegevens geoorloofd zijn. Als de gegevens echter verplicht zijn verstrekt voor geheel andere doeleinden, zal veel eerder sprake zijn van onverenigbaarheid.

[Voor het verkrijgen van de persoonsgebonden clubcard van de KNVB was het verplicht naam, adres en woonplaats op te geven. Die gegevens werden geregistreerd ten behoeve van de handhaving van de openbare orde. Commercieel gebruik van die gegevens is in dat geval niet verenigbaar.]

Ook overheidsinstellingen hebben soms behoefte om bepaalde producten of diensten onder de aandacht te brengen. Pro-actieve dienstverlening lijkt vooral bij armoedebestrijding een aantrekkelijk instrument. Waar het tot de taak van het betreffende overheidsorgaan behoort of in het verlengde ligt van de uitvoering van een wettelijke regeling, om de burger te wijzen op bepaalde rechten, is de grondslag voor dit gebruik direct gelegen in de taakuitoefening door het betreffende overheidsorgaan. Als gegevens die zijn verzameld in het kader van de uitvoering van een wettelijke regeling worden gebruikt voor verdergaande pro-actieve dienstverlening, gaat het om verder gebruik dat verenigbaar dient te zijn met het doel waarvoor de gegevens zijn verzameld en vervolgens geregistreerd. Dit dient te worden beoordeeld aan de hand van de hiervoor vermelde criteria (98.V.0874).
Selecteren en verenigbaar gebruik

Het bedrijf dat een mailing doet uitgaan zal vanuit een oogpunt van efficiency en kostenbeheersing deze bij voorkeur richten tot een doelgroep die potentieel geïnteresseerd is. Die interesse is af te leiden uit gegevens als leeftijds- of inkomensklasse en afname van

bepaalde verwante producten. Het maken van een selectie aan de hand van dergelijke gegevens is daarbij een veel toegepaste techniek. Die techniek is bruikbaar in het kader van werving voor commerciële en charitatieve doeleinden, maar ook voor geheel andere doeleinden. Het is immers ook mogelijk om aan de hand van bepaalde factoren selecties te maken van personen bij wie sprake is van bepaalde risico's, van wie bepaalde gedragingen of transacties aanleiding geven tot een vermoeden van fraude, of die mogelijk in aanmerking komen voor bepaalde subsidies of uitkeringen. Vanuit genoemde overwegingen van efficiency en kostenbeheersing lijkt het maken van bepaalde selecties de moeite waard als het gaat om risicoselectie, fraudebestrijding of pro-actieve dienstverlening door de overheid.

Bij het maken van selecties gaat het meestal om gebruik van gegevens voor een ander doel dan waarvoor ze oorspronkelijk zijn verkregen en geregistreerd. De vraag of dit gebruik verenigbaar is met het doel van de registratie doet zich ook hierbij voor. De al eerder genoemde wegingsfactoren spelen hierbij een rol. Het maken van een selectie ten behoeve van een mailing aan de hand van verplicht verstrekte inkomensgegevens zal bijvoorbeeld eerder als 'onverenigbaar gebruik' moeten worden betiteld dan wanneer de betrokkene de keuze heeft gehad deze gegevens wel of niet te verstrekken. Daarnaast kan ook de bij het selecteren gevolgde werkwijze van belang zijn. Zo dient bij het analyseren van declaratiegegevens van patiënten door een verzekeraar met als doel het vaststellen van significant afwijkende kosten per zorgverlener te worden gekozen voor een methode van onderzoek die het minst ingrijpt in de persoonlijke levenssfeer. Bijvoorbeeld door in beginsel gebruik te maken van geanonimiseerde gegevens en slechts indien noodzakelijk van gecodeerde c.q. identificerende gegevens. Ook is van belang dat tevoren is vastgesteld wanneer van 'significant afwijkende kosten' gesproken kan worden. Het geven van goede informatie over het onderzoek en de mogelijke gevolgend daarvan, tenslotte, is essentieel (97.K.368)

[De selectie door een pensioenfonds van alle geregistreerden die in het onderwijs werkzaam zijn geweest, voor een mailing waarin ze worden gewezen op de mogelijkheid om een bijdrage te leveren aan de oplossing van een personeelstekort in het onderwijs, lijkt op het eerste gezicht geen 'verenigbaar gebruik' van die persoonsgegevens. Het betrof echter een eenmalige actie van de staatssecretaris van onderwijs, waarbij het uitsluitend ging om naam- en adresgegevens zonder verdere selectiekenmerken van de geregistreerden. Gezien hun oud-werknemerschap in het onderwijs werd hun affiniteit met die sector verondersteld, en was er voldoende reden om hen te informeren over een voor hen interessante ontwikkeling. Alternatieve methoden waren niet zomaar voorhanden en het ging om een belangrijk maatschappelijk belang. De Registratiekamer achtte de actie op grond van die overwegingen niet in strijd met de WPR.]

Privatisering en verenigbaar gebruik

De vraag in hoeverre gegevens die door de geregistreerde verplicht zijn verstrekt, verder kunnen worden gebruikt in het kader van commerciële doelstellingen, doet zich nu al voor binnen die concerns en bedrijven waar de nog 'publieke' taken op het terrein van de sociale zekerheid worden uitgevoerd naast 'private', commerciële activiteiten. Concerns bijvoorbeeld waarvan naast uitvoeringsinstellingen ook Arbo-diensten en verzekeringsmaatschappijen deel uitmaken, maar ook assurantietussenpersonen die werkgevers aanbieden om het complexe geheel van gegevensverwerkingen dat het gevolg is van de privatisering in de sociale zekerheid voor hen uit te voeren.

In een advies over de gewenste toekomstige ontwikkeling van de Organisatiewet sociale verzekeringen (OSV) bepleitte de Registratiekamer een duidelijke grensafbakening in de wet voor wat betreft het commerciële (neven)gebruik van persoonsgegevens (98.A.0459). In het kabinetsstandpunt over de toekomstige Structuur Uitvoering Werk en Inkomen (SUWI) is aangegeven dat uitvoeringsinstellingen persoonsgegevens slechts voor andere doeleinden dan de uitvoering van werknemersverzekeringen zullen kunnen gebruiken, als die doeleinden daarmee verenigbaar zijn. Als een voorbeeld van onverenigbaar gebruik wordt in dit verband vermeld het gebruik van in het kader van werknemersverzekeringen verzamelde gegevens bij de aanvraag van een levensverzekering.

Samenwerking en verenigbaar gebruik

Op allerlei terreinen werken organisaties steeds meer samen om gerechtvaardigde doelen te realiseren. De effectieve uitvoering van de werkzaamheden staat daarbij steeds voorop. De samenwerking krijgt voor wat betreft de omgang met persoonsgegevens verschillende vormen. Samenwerking leidt vaak tot het samenvoegen van gegevensverzamelingen. Ook kan het wenselijk worden geacht om allerlei persoonsregistraties met elkaar te koppelen. Daarbij kan het gaan om vergelijking van persoonsgegevens in verschillende registraties, maar ook om een gestructureerde gegevensuitwisseling te realiseren, al dan niet volgens een vooraf vastgestelde berichtenstructuur. Bij het voorkomen en bestrijden van specifieke vormen van criminaliteit zoals fraude, milieudelicten en extreme overlast, werkt de politie steeds vaker samen met ambtenaren van controlerende diensten en bijzondere opsporingsdiensten of met functionarissen uit de gezondheidszorg en de maatschappelijke dienstverlening. Met het oog op het voorkomen en bestrijden van deze criminaliteit worden handhavingsteams opgericht in allerlei soorten en maten. Een voorbeeld hiervan is het Regionaal Interdisciplinair Fraudeteam (RIF) ter opsporing van ‘zwarte fraude’ door werkgevers en personen die een uitkering genieten. De Registratiekamer heeft vuistregels voor een RIF ontwikkeld. Enkele hiervan zijn: (i) duidelijkheid over de formele en feitelijke verantwoordelijkheid (beheersniveau); (ii) een duidelijke scheiding tussen controle- en opsporingsactiviteiten; (iii) participanten moeten handelen binnen hun eigen bevoegdheid; (iv) het bestaan van een privacyreglement waarin voorlichting en interne normering wordt gegeven; (v) heldere formulering doel van een RIF; (vi) een deugdelijke en inzichtelijke wijze waarop met de verkregen persoonsgegevens wordt omgegaan.

Een ander voorbeeld van samenwerking betreft het opsporen van onrechtmatige bewoning. De staatsecretaris van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer legde de Registratiekamer ter advisering de aanbevelingen voor van het rapport *Onrechtmatige bewoning en het raadplegen van bestanden* van de Commissie Zwart. Deze commissie ging ervan uit dat bestanden van allerlei organisaties onderling toegankelijk konden worden gemaakt. Alleen de wijze waarop gegevens worden uitgewisseld zou problemen kunnen opleveren. De Registratiekamer heeft erop gewezen dat het onderling toegankelijk maken en het vergelijken van gegevens uit bestanden een vorm van gegevensverstrekking is waarvoor bij of krachtens (inter)nationale wetgeving voorwaarden gelden. Dat betekent niet dat gegevensuitwisseling niet mag plaatsvinden, maar wel dat het regime van de samenwerking steeds weer zorgvuldig dient te worden bepaald. De hierboven genoemde vuistregels bij het RIF zijn ook in dit verband relevant. In zijn reactie heeft de staatssecretaris het standpunt van de Registratiekamer overgenomen. Dit betekent dat op een vanuit privacybescherming

verantwoorde wijze kan worden opgetreden tegen het groeiende verschijnsel van illegale bewaring in met name de sociale sector.

De twee hierboven geschetste gevallen van veelal publiekrechtelijke burenhulp zijn gericht op controle op de door de burgers overgelegde gegevens en het inlichten van elkaar van fraudegevallen. Dat deze publiekrechtelijke burenhulp ook op meer positieve wijze wordt ingezet blijkt uit de nota van de minister van Binnenlandse Zaken en Koninkrijkrelaties over de pro-actieve dienstverlening door de overheid. Vele subsidies van de overheid bereiken de burger niet, ondanks de voorlichting die darover wordt gegeven. Dat kan zijn huursubsidie, bijzondere bijstand, kwijtschelding van gemeentelijke belastingen of gemeentelijke kortingsregelingen. Door bestandsvergelijking wil de overheid de burger actief en persoonlijk benaderen. De Registratiekamer heeft in haar advies erop gewezen dat bij pro-actieve dienstverlening ook de wettelijke spelregels moeten worden gevolgd. Er wordt te gemakkelijk gesproken over het koppelen van gegevens in het belang van de burger. Koppeling van bestanden wordt te vaak als enige oplossing gezien. Een actieve overheid kan ook op alternatieve manieren de burger wijzen op zijn rechten, bijvoorbeeld door het meesturen van voorlichtingsmateriaal in het normale contact met de burger. Het te dicht de burger op de huid komen kan ook een averechts effect hebben. Actieve voorlichting moet niet in armoede-recherche ontaarden.

Een voorbeeld waarin sprake is van een gestructureerde gegevensuitwisseling in een samenwerkingsverband zijn pilots in de sociale zekerheid. De Arbeidsvoorziening, de uitvoeringsinstanties (UVI's) en de gemeentelijke sociale diensten zijn in enkele plaatsen een samenwerkingsverband aangegaan om de gegevensuitwisseling tussen de organisaties te standaardiseren en te structureren. Uitgangspunt daarbij is dat de werkloze zo snel mogelijk weer naar de arbeidsmarkt wordt geleid en dat hij zijn persoonsgegevens bij het begin van zijn werkloosheid slechts bij één loket hoeft te overleggen waarna zijn uitkeringsaanvraag verder wordt verwerkt. Hiervoor is het Cliënt Volg Communicatie Stelsel (CVCS) ontwikkeld: een computerprogramma met een gestructureerde en gestandaardiseerde gegevensuitwisseling met behulp van EDI-berichten en bepaalde meldingen aan de samenwerkende organisaties. De sturing en begeleiding van dit project vindt plaats door de Stichting CVCS. Het is de bedoeling dat op termijn dit systeem landelijk wordt ingevoerd. Bijzondere aandacht bij dit project behoeft naast de wettelijke grondslag voor de gegevensuitwisseling, de zorgvuldigheid, de beheersbaarheid, de controleerbaarheid en de beveiliging van de gegevensuitwisseling met het oog op de bescherming van de persoonlijke levenssfeer. In 1999 zal de Registratiekamer zich hierover uitspreken op basis van de resultaten van een evaluatieonderzoek dat wordt verricht door de Stichting CVCS.

5.3 Technology Assessment

Technology assessment stelt de Registratiekamer in staat de kritieke momenten in de ontwikkelingen en toepassingen van informatie- en communicatietechnologie in beeld te brengen. Welke technologieën zijn privacybedreigend en welke privacybevorderend? Hoe kunnen de normen van gegevensbescherming in de techniek een vertaling vinden? De opvolging van de huidige Wet persoonsregistraties (1989) door de Wet bescherming persoonsgegevens is onder meer ingegeven door de sterk veranderde aard en inzet van informatie- en communicatietechnologie. Waar in de tachtiger jaren 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 *verwerking* van persoonsgegevens: alle mogelijke processen die met persoonsgegevens worden verricht, van het moment van genereren of vergaren tot en met het moment waarop de gegevens vernietigd worden.

Privacy Enhancing Technologies

Een belangrijke denkrichting die de Registratiekamer stimuleert is de inzet van technologieën die bijdragen aan het verminderen van de hoeveelheid persoonsgegevens die binnen informatiesystemen worden verwerkt. In conventionele informatiesystemen worden veelal grote hoeveelheden informatie over personen vastgelegd, waaronder ook gevoelige gegevens. Door de steeds groeiende mogelijkheden van computers en netwerken worden steeds vaker koppelingen aangebracht met andere persoonsgegevens, waardoor het gehalte aan informatie over personen binnen de systemen exponentieel groeit. Om dit te voorkomen dienen informatiesystemen te worden aangepast. In 1998 is het eerder door de Registratiekamer samen met haar Canadese zusterorganisatie uitgebrachte rapport *Privacy enhancing technologies: the path to anonymity* geactualiseerd en herdrukt. Dit rapport geeft mogelijkheden om met behulp van informatietechnologie het aantal persoonsgegevens binnen een systeem te beperken, dan wel de opname van nieuwe –niet essentiële – persoonsgegevens te voorkomen, zonder dat de gewenste functionaliteit van het systeem wordt aangetast.

De belangrijkste optie is bij het gebruik geen enkel identificerend persoonsgegeven te genereren of vast te leggen. De afwezigheid van identificerende data en datasporen maakt het in veel gevallen 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 adequaat te beschermen. Bij ieder gebruik van het systeem wordt de identiteit van de gebruiker omgezet in een, voor elke transactie unieke, pseudo-identiteit. De privacy van geregistreerde wordt zo afdoende beschermd. Hierbij kan gebruik gemaakt worden van bestaande technieken zoals versleuteling, digitale handtekeningen en Trusted Third Parties. De belangstelling voor dit 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 in de praktijk vaak 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 is verheugend dat het initiatief tot het implementeren van *privacy-enhancing technologies* (PET) steeds vaker door en binnen diverse branches zelf wordt genomen. De Registratiekamer is in 1998 om advies gevraagd door onder meer bouwers van medische informatiesystemen, systemen voor biometrische identificatie en dataminingtools.

Datamining en datawarehousing

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 de 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 persoonsgegeven in *datawarehouses* en *datamining* om te zoeken naar niet eerder vastgestelde samenhangen binnen die gegevens. Datawarehousing en datamining, samen aangeduid als knowlegde discovery in databases (KDD) zijn door de Registratiekamer onderkend als belangwekkende trends. Binnen het technology assessment programma is in 1998 een studie gedaan naar de privacy aspecten van deze technieken. De resultaten zijn neergelegd in de publicatie *Gouden bergen van gegevens*.

Software agents

Samen met TNO/FEL is in het afgelopen jaar een studie afgerond over intelligent software agents and privacy. Een agent is een software programma dat min of meer zelfstandig taken kan uitvoeren voor zijn opdrachtgever. Agents 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 assistentie wegwijs te worden in de grote hoeveelheden informatie die zich op grote computernetwerken bevinden. Zoekmachines op het Internet zijn de 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. De publicatie *Intelligent software agents and privacy* is begin1999 uitgebracht in samenwerking met de Canadese tegenhanger van de Registratiekamer, de Information and Privacy Officer in Ontario. In het rapport worden de thans in ontwikkeling zijnde agents geïnventariseerd, alsmede de privacyaspecten wanneer deze hun eigenaar vertegenwoordigen. Tot slot bevat het rapport een aantal modellen aan de hand waarvan het PET-principe kan worden verwerkt in de bouw van agents. Inzake de privacy aspecten van software agents werd advies uitgebracht aan de Telecommunicatie expertgroep van de EU-werkgroep van nationale toezichthouders op het terrein van de privacybescherming, als bedoeld in artikel 29 van de Europese richtlijn nr. 95/46/EG.

Biometrische identificatie

Een van de significante ontwikkelingen in 1998 op het terrein van informatie- en communicatietechnologie is de doorbraak van systemen voor biometrische identificatie en authenticatie. 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, bijvoorbeeld 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 het risico van fraude of onbevoegd gebruik.

Vanuit privacyoogpunt plaatst de Registratiekamer de nodige kanttekeningen bij grootschalige invoering van biometrische systemen. Het unieke karakter van lichaamskenmerken houdt tevens een dreiging in. Wanneer zij 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 stemherkenning over telecommunicatie verbindingen, staat tevens de mogelijkheid van anonieme communicatie 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 is de Registratiekamer samen met TNO/FEL een studie gestart 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, waarop de Wet bescherming persoonsgegevens is gebaseerd.

Informatiebeveiliging

In 1998 is de beveiliging van persoonsgegevens een belangrijk punt van aandacht en zorg gebleven. De sterk voortschrijdende netwerktechnologie en de daardoor ontstane mogelijkheden voor transport en koppeling van gegevens, zetten veel organisaties, binnen overheid en bedrijfsleven aan tot ambitieuze samenwerkingsverbanden. De beveiliging van gegevens houdt vaak geen tred met die ontwikkelingen zodat aanzienlijke risico’s ontstaan voor het onbevoegd gebruik van persoonsgegevens. In de privacy-audits die de Registratiekamer in 1998 uitvoerde (zie 5.4) is dat meer dan eens gebleken.

De publicatie *Beveiliging Persoonsregistraties*, waarin normen voor de informatiebeveiliging worden gegeven gebaseerd op artikel 8 van de WPR, is in 1998 herzien. In de nieuwe versie is rekening gehouden met recente ontwikkeling binnen de informatie- en communicatietechnologie, met name het gebruik van netwerken. De nieuwe normen zijn in lijn met de *state-of-the-art* op het gebied van informatiebeveiliging. Ook is het nieuwe advies afgestemd op de in het bedrijfsleven gehanteerde *Code voor Informatiebeveiliging* en het voor de rijksoverheid geldende *Voorschrift Informatiebeveiliging*. Het advies zal worden afgestemd op de Wet bescherming persoonsgegevens.

5.4 Handhaving

Als toezichthouder heeft de Registratiekamer een aantal instrumenten tot haar beschikking om naleving van de wettelijke bepalingen te bevorderen. De Registratiekamer kan de aanmeldingen van persoonsregistraties (marginaal) toetsen. In geschillen over inzage, correctie en verwijdering van persoonsgegeven, kan de Registratiekamer bemiddelen en naar aanleiding van andere klachten een onderzoek instellen. Met het uitvoeren van privacy-audits

onderzoekt en beoordeelt de Registratiekamer inhoeverre bepaalde informatiesystemen waarin persoonsgegevens worden verwerkt, voldoen aan de wettelijke normen.

Aanmeldingen

Personen of instanties die een persoonsregistratie voeren (registratiehouders) zijn in principe verplicht dat te melden bij de Registratiekamer. Dit gebeurt via een aanmeldingsformulier waarin onder andere wordt aangegeven wat het doel is van de persoonsregistratie, welke gegevens worden vastgelegd, wie de gegevens gebruikt en waarvoor ze gebruikt worden. Overheidsorganisaties, andere organisaties die met de uitvoering van overheidstaken zijn belast en instellingen voor onderwijs, gezondheidszorg en maatschappelijke dienstverlening moeten voor elke persoonsregistratie een privacy-reglement vaststellen. De aanmelding en het reglement zorgen ervoor dat het gebruik van gegevens transparant wordt voor de geregistreerde. Deze kan namelijk aan de hand van het aanmeldingsformulier of het reglement zien welke gegevens er verzameld worden en hoe een organisatie daarmee omgaat.
De Registratiekamer toetst de aanmeldingsformulieren marginaal. Bij de behandeling van klachten is het aanmeldingsformulier van de betrokken organisaties een belangrijk document.

Eind 1997 waren in totaal 57.786 bestanden bij de Registratiekamer aangemeld en in 1998 werden daar 3.325 bestanden aan toegevoegd. (zie bijlage 1). De aanmeldingsplicht of de plicht een privacy-reglement op te stellen geldt niet voor alle persoonsregistraties. In het Besluit genormeerde vrijstelling is vastgelegd voor welke typen registraties een vrijstelling geldt en onder welke voorwaarden. De Wet persoonsregistraties blijft overigens wel van toepassing op registraties die zijn vrijgesteld van de aanmeldingsplicht.

Bemiddeling en klachtenbehandeling

Op grond van de Wet persoonsregistraties (WPR) en de Wet politieregisters (WPOLR) kan iemand over wie gegevens in een bestand zijn opgenomen, de Registratiekamer verzoeken te bemiddelen wanneer hij/zij een conflict heeft met de verantwoordelijke voor dat bestand. Dit conflict kan gaan over de uitoefening van het recht tot inzage in de gegevens of de verstrekking van een afschrift en de kosten die daarvoor in rekening worden gebracht. Het kan ook gaan over een verzoek om verbetering of verwijdering van gegevens van de betrokkene, waaraan geen gehoor wordt gegeven. De Registratiekamer kan op verzoek van een belanghebbende ook een klacht onderzoeken over de rechtmatigheid van de inrichting en het gebruik van een persoonsregistratie. Vaak gaat het daarbij om klachten over het al dan niet terecht verstrekken van gegevens aan derden.

Bij de beoordeling van een verzoek om bemiddeling of het onderzoeken van een klacht onderzoekt de Registratiekamer of de klager ontvankelijk is en de behandeling opportuun. Er moet sprake zijn van een persoonsregistratie waarop de WPR van toepassing is en de klager moet het probleem al hebben voorgelegd aan de verantwoordelijke organisatie. Ook wordt gekeken of er binnen de betreffende sector een klachtenregeling geldt die eerst doorlopen dient te worden en of de zaak niet in behandeling is bij een rechterlijke instantie. Sommige verzoeken kunnen beter door andere instanties behandeld worden, waarbij de Registratiekamer op de achtergrond van advies dient. Dit is bijvoorbeeld het geval wanneer een patiënt inzage vraagt in een medisch dossier, omdat hij/zij ontevreden is met de

behandeling. De Registratiekamer kan wel bemiddelen wat betreft het inzagerecht, maar geen uitspraak doen over de kwaliteit van de behandeling. Door deze beperkte bevoegdheden is de Registratiekamer niet altijd in staat om een conflict geheel op te lossen, terwijl andere instanties (zoals een Informatie- en Klachtenbureau Gezondheidszorg) dat wel doen. Door met deze instanties contacten te leggen en te onderhouden, zorgt de Registratiekamer ervoor dat er zoveel mogelijk gebruik gemaakt wordt van de kennis die daar voorhanden is. In de meeste gevallen is een uitspraak van de Registratiekamer voldoende om een conflict te beëindigen. Wanneer dit niet het geval is, staat voor de verzoeker de weg naar de rechter open.

Klachten worden soms telefonisch afgehandeld, maar meestal is een verdergaand onderzoek vereist en wordt het probleem voor een reactie voorgelegd aan de andere partij. Dit is vaak een schriftelijke procedure. Het beginsel van hoor en wederhoor is voor de Registratiekamer standaard in de behandeling van klachten en geschillen. De Registratiekamer heeft voor het doen van een onderzoek naar aanleiding van een klacht, bijzondere bevoegdheden: de registratiehouder moet inlichtingen geven en alle overige medewerking verlenen. Een onderzoek kan leiden tot een openbaar rapport.

In 1998 bemiddelde de Registratiekamer bij 108 conflicten (tegenover 136 in 1997). Vaak onstonden conflicten doordat geweigerd werd om inzage te verlenen of te hoge kosten berekend voor het verstrekken van een kopie van een dossier. Ook lijken sommige direct marketeers zich weinig aan te trekken van een verzoek om verwijdering van gegevens waardoor mensen nog steeds ongewenste reclame ontvangen. 211 klachten werden onderzocht (tegenover 238 in 1997). Een aantal van deze klachten had betrekking op handelsinformatiebureaus. Deze bureaus verzamelen gegevens om de kredietwaardigheid van verschillende groepen te kunnen bepalen. Ook mobiele telefoonaanbieders maken gebruik van deze handelsinformatiebureaus. Uit de reacties bleek dat voor de consument vaak niet duidelijk is waar de door een handelsinformatiebureau en een telecom-aanbieder gebruikte gegevens vandaan komen. Ook waren er klachten over sociale diensten die uitkeringsgerechtigden meer vragen dan nodig is om te het recht op en de hoogte van de uitkering vast te stellen.

[Voorkomen is beter dan genezen. Behalve de klachten en geschillen, behandelde de Registratiekamer in 1998 ook 595 schriftelijke verzoeken om advies en voorlichting inzake het gebruik van persoonsgegevens en het (her)inrichten van systemen.]

Audits

De Registratiekamer doet niet alleen onderzoeken naar aanleiding van klachten, maar ook op eigen initiatief. Een privacy-audit is zo’n onderzoek. Hierbij wordt gebruik gemaakt van inzichten die binnen het vakgebied Electronic Data Processing-auditing (EDP-auditing) gelden. Het doel van een privacy-audit is het geven van een oordeel en aanbevelingen over de kwaliteit van de bescherming van de persoonsgegevens. Dit gebeurt door middel van een beoordeling van de opzet en de werking van maatregelen en procedures die in relatie met privacybescherming zijn gerealiseerd. Kwaliteitsaspecten die hierbij een rol spelen zij integriteit, exclusiviteit en beschikbaarheid.

De Registratiekamer verrichtte onderzoek naar de kwaliteit van privacybescherming van de personen van wie gegevens zijn opgenomen in het Nationaal Schengen Informatiesysteem

(NSIS). Het NSIS is het Nederlandse deel van het Schengen Informatiesysteem (CSIS). Hierin worden gegevens opgenomen van mensen die niet zonder meer een grens van een van de Schengenlanden (Benelux, Duitsland, Frankrijk en Italië) mogen overschrijden. Omdat de in het NSIS opgenomen gegevens gevoelig zijn, is het van groot belang dat hiermee zorgvuldig wordt omgegaan. De Registratiekamer verheugde zich in de constructieve medewerking van de betrokken instanties, maar constateerde wel een groot aantal tekortkomingen in de fysieke, logische en organisatorische beveiliging van de persoonsgegevens in het NSIS. De meeste van deze tekortkomingen zijn inmiddels al verholpen doordat de betrokken instanties de aanbevelingen van de Registratiekamer hebben opgevolgd. De Registratiekamer verrichte op soortgelijke wijze een privacy-audit bij de gemeentelijke basisadministratie (voorheen het bevolkingsregister) van de gemeenten Almelo, Breda en Langedijk, waarvan de resultaten in 1999 zijn gepubliceerd.

Gezien de ontwikkelingen binnen de informatie- en communicatietechnologie en de toenemende internationalisering van gegevensverkeer, acht de Registratiekamer samenwerking op het gebied van privacy-audits met zusterinstellingen van groot belang. Daarom is in 1998 de voorbereiding gestart voor een privacy-audit in samenwerking met de Spaanse zusterorganisatie: *Agencia de Protección de Datos.* In 1998 werd ook gewerkt aan de bevordering van zelfregulering door samen te werken met het Koninklijk Nederlands Instituut van Registeraccountants en de Nederlands Organisatie voor Register EDP-auditers, met name in verband met de invoering van de toekomstige Wet bescherming persoonsgegevens.

6 Organisatie

In 1997 startte de Registratiekamer met het verder professionaliseren van de organisatie. In 1998 werd dat traject voorgezet. Een onderdeel daarvan was de inrichting van een *front-office*, waarin de bulk van eenvoudige zaken (klachten, bemiddelingsverzoeken en adviesverzoeken) op gestandaardiseerde wijze wordt afgehandeld. Daarmee is een belangrijke voorwaarde vervuld om meer beleidsmedewerkers in te zetten voor onderzoeksprojecten. Om het reeds ontwikkelde beleid op het terrein van *EDP-auditing* en *technology assessment* te consolideren en verdere activiteiten te ontwikkelen, is in 1998 een unit ingericht, bestaande uit twee auditors, een technologie medewerker en een informatica specialist.
Ten behoeve van de voortgangsbewaking en procesbesturing, is in 1998 een systeem ontwikkeld voor documentmanagement, dat in 1999 operationeel zal zijn. In het kader van de professionalisering is in 1998 een onderzoek gedaan naar de kwaliteit van de dienstverlening door de afdeling automatisering, het bedrijfsbureau, administratie, receptie en bibliotheek. Het interne beveiligingsplan is in 1998 geactualiseerd.

Het materiële budget bedroeg in 1998 *f* 1.003.600 exclusief huurkosten en exclusief een extra bijdrage van *f* 250.000 ter voorbereiding van de invoering van de Wet bescherming persoonsgegevens (WBP). Het personele budget bedroeg *f* 4.169.100. Aan de formatie is in 1998 1,5 fte beleidsmedewerker, 1 fte administratieve ondersteuning en 1 fte voorlichting toegevoegd. De beschikbare formatie was per 31 december 1998 43 fte. De feitelijke bezetting per die datum was 41,5 fte, waarvan 25 mannen en 22 vrouwen. In de loop van het jaar verlieten zes medewerkers de Registratiekamer en traden elf nieuwe medewerkers in dienst. Het ziekteverzuim bedroeg in 1998 4.8% (tegenover 7.2% in 1997).

Ondernemingsraad

De ondernemingsraad is in 1998 nauw betrokken geweest bij de de reorganisatie van de Registratiekamer en de gesignaleerde knelpunten op het terrein van informatievoorziening, personeelsbeleid en de (her)inrichting van de verschillende functies binnen de Registratiekamer. Samen met de leiding is gewerkt aan een kwaliteitsverbetertraject. Dit traject is gebaseerd op het model van het Instituut Nederlandse Kwaliteit, het INK-model, dat binnen de overheid en bedrijfsleven op steeds grotere schaal ingang vindt.

Bijlage 1 Persoonsregistraties aangemeld bij de Registratiekamer per 31 december 1998 gespecificeerd naar sector

Landbouw en visserij	7
Delfstoffenwinning	3
Uitgeverijen	85
Geneesmiddelenfabrieken	125
Industrie overig	235
Sociale werkplaatsen	55
Nutsbedrijven	100
Bouwnijverheid	35
Auto- en garagebedrijven	3217
Apothekers	1095
Postorderbedrijven	71
Opticiëns	540
Handel overig	372
Goederenvervoer	34
Personenvervoer	48
Luchtvaartmaatschappijen	11
Verkeers- en toeristenbureau's	20
Post- telefoon- en telegraafdiensten	57
Transport/opslag/communicatiebedrijv.overig	60
Beleggingsmaatschappijen	23
Banken	1719
Hypotheekbanken	21
Financieringsbemiddeling	545
Creditcardorganisaties	15
BKR	2
Bankwezen overig	112
Ziektekostenverzekeringen	144
Levensverzekeringen	62
Schadeverzekeringen	184
Pensioenfondsen	47
Assurantiebemiddeling	4795
Verzekeringswezen overig	459
(Woningbouw)verenigingen/stg/co”peraties	1020
Eigenaarsverenigingen	5
Makelaarskantoren	255
Exploitatie/handel onroerend goed overig	39
Rechtskundige diensten	14
Advokaten	78
Rechtskundige adviesbureau's	9
Notarissen	76
Deurwaarders	79
Accountantburo's	44
Boekhoudburo's en administratiekantoren	98
Belastingadviesburo's	27
Accountants-/boekhoudbureau's etc. overig	66

Computercentra en softwarebureau's	31
Reclame-, advertentiebureau's e.d.	9
Direct marketing	453
Telemarketing	8
Economisch adviesbureau's	89
Persbureau's, nieuwsbureau's	3
Uitzendbureau's	426
Arbeidsvoorziening	32
Arbeidsbemiddeling/Werving en Selectie	1385
Uitzend-/uitleenbedrijven arbeidsbem.overig	600
Bureau's psychotechnische personeelstesten	19
Informatiebureau's	8
Incassobureau's	3
Recherche- c.q. detectivebureau's	373
Kredietinformatiebureaus (personen)	14
Handelsinformatiebureaus (bedrijven)	16
Bewaking- en beveiligingsdiensten	95
Zakelijke dienstverlening overig	233
Verhuur machines + andere roerende goederen	32
Overheid algemeen	66
Rijksoverheid	586
Provinciale overheid	269
Gemeentelijke overheid	13738
Intergemeentelijke samenwerkingsverbanden	37
Waterschappen	167
Rechterlijke macht	100
Openbaar Ministerie	69
Gevangeniswezen	124
TBR/TBS kliniek	7
Kinderbescherming	69
Reclassering	11
Rechterlijke org,gevangenisw.,reclass. ov.	13
Politie	675
Bijzondere opsporingsdiensten	50
Ziekenfondsen	91
Bedrijfsverenigingen	30
Sociale Verzekeringsraad	6
Sociale fondsen	16
Uitvoeringsorganen sociale zekerheid overig	39
Overige dienstverlening	13
Kerkgenootschappen	18
Religieuze/levensbeschouwelijke org. Overig	12
Basisonderwijs	83
Middelbaar onderwijs	114
Hoger onderwijs	32
Schoolbegeleidings-/adviesdienst (SBD/SAD)	47
Universiteiten	69
Type- en computercursussen	1
Onderwijs overig	153

Ziekenhuizen	2208
Psychiatrische Ziekenhuizen/inrichtingen	341
Verpleeghuizen	781
GG&GD	523
Bedrijfsgezondheidszorg (BGD's)	292
Revalidatiecentra	73
Bloedbanken	45
Kruiswerk/thuiszorg/kraamzorg	745
Medische instellingen overig	493
Huisartsenpraktijken	3767
Overige artsen (niet specialisten)	76
Internist	20
Psychiater	70
Oogarts	41
KNO-arts	20
Dermatoloog	33
Zenuwarts	26
Overige specialisten-praktijken	167
Tandartsenpraktijken	2376
Fysiotherapeuten	3396
Mensendieck/Cesar	654
Pedicures/manicures/voetverzorging	154
Overige (para)medische behandelaars	373
Dierenartsen	27
Logopedisten	1112
Diëtisten en voedingskundigen	160
Verloskundigen	249
Psychotherapeuten	95
Gezondheidszorg overig	132
Verzorgings- en bejaardentehuizen	2362
Verblijven geestelijk/lichamelijk gehandic.	443
Soc.-medische/psychologische/pedagog. dnst	148
Hulpinstellingen bij verslaving	57
RIAGG'S	84
Gezinsverzorging en gezinshulp	75
Vluchtelingenwerk	266
Dagverblijven voor kinderen	152
Relatiebemiddeling	212
Maatschappelijke dienstverlening overig	794
Buurt/clubhuis,jongeren/opbouw/vormingswerk	19
Bibliotheken	7
Arthoteken	2
Musea	16
Media	6
Sociaal-culturele-/culturele inst. overig	65
Sport en vrijetijdsbesteding	358
Kamers van Koophandel	42
Researchinstellingen	319
Publiekrechtelijke bedrijfsorganisaties	30

Vakbonden	14
Belangenverenigingen	232
Politieke partijen	6
Bedrijfs-/werknemerorganisaties etc. overig	13
Begrafenis-, uitvaartondernemingen	194
Overige dienstverlening (overig)	48
Overig	59
TOTAAL	61111

Bijlage 2 Adviezen

Adviezen aan de regering uitgebracht in 1998

[Alle adviezen kunt u aanvragen bij de Registratiekamer. Tekst en/of samenvatting van de meeste adviezen kunt u ook vinden op de website www.registratiekamer.nl]

Aanpassing van de telecommunicatiewet aan de WBP
3 november 1998

Aanwijzing stichting FVP
11 september 1998

Wetgeving electronische snelweg
1 september 1998

Mededelingen over antecedenten uit politieregisters
9 juli 1998

Claimbeoordeling door publieke instelling
26 juni 1998

Taakstelling regionale commissie van toezicht politie
23 juni 1998

Koppelingswet vreemdelingen/GBA
3 juni 1998

Privacybescherming en RINIS
15 mei 1998

Visienota justitiële gegevens
11 mei 1998

Gebruik persoonsgebonden nummer in onderwijs
28 april 1998

Encryptie niet aan banden leggen
9 april 1998

Gerechtsdeurwaarders en electronische gegevensuitwisseling
20 maart 1998

Toegang tot personeelsdossiers
13 maart 1998

Kritiek op telecommunicatiewet
9 maart 1998

Wetsvoorstel Computercriminaliteit II
9 maart 1998

Aanpassing Wet GBA aan Europese richtlijn
26 februari 1998

Wijziging Wet GBA
26 februari 1998

Personeels-informatiesysteem politie
19 februari 1998

Adviezen aan de regering uitgebracht in de periode 1997-1990

Registratie van prepaid telefoonkaarten
12 december 1997

Telecommunicatiewet
13 november 1997

Wetsvoorstel Rekening rijden
31 oktober 1997

Verzamelwet GBA
15 oktober 1997

Wetsontwerp Bevordering integere besluitvorming openbaar bestuur (BIBOB*)*
14 oktober 1997

Koppelingswet
16 september 1997

Wijziging Besluit verstrekking gegevens telecommunicatie
12 september 1997

Alarmnummer 1-1-2
12 september 1997

Wijziging Besluit gebruik sofi-nummer
28 augustus 1997

Bijzondere politieregisters
26 augustus 1997

Wetsvoorstellen nummeridentificatie
18 juli 1997

Bijzondere opsporingsbevoegdheden
13 maart 1997

Wet bescherming persoonsgegevens
februari 1997

Informatieverstrekking aan ziekenfondsverzekerden i.v.m. eigen bijdrage
7 februari 1997

Besluit politieregisters en informatieverstrekking aan financiële toezichthouders
31 januari 1997

Wijziging Wet politieregisters
22 november 1996

Informatiebeveiliging politie
15 november 1996

Politiedatacommunicatienetwerk Podacs en landelijke opsporingsdiensten
25 oktober 1996

Sofinummer in het onderwijs
13 september 1996

Aanpassing Afbakeningsbesluit
26 augustus 1996

Penitentiaire maatregel
2 augustus 1996

Wijziging besluit politieregisters
9 juli 1996

Wijziging WPR en WPOLR
9 juli 1996

Reglement verpleging ter beschikking gestelden
1 juli 1996

Amerikaans voorstel tot uitgifte van een TIN
(Taxpayer Identification Number for Foreign Persons)
28 juni 1996

Rapportage bejegeningsgegevens
29 januari 1996

Nummeridentificatie bij 06-11 alarmcentrales
7 november 1995

Uitbreiding gebruik Sofinummer
3 november 1995

Medische zorgpas
5 oktober 1995

Wijziging Wet op de ondernemingsraden
20 september 1995

Invoering Wet PEMBA en WAZ
11 september 1995

Wijziging Besluit GBA in verband met onderzoek baarmoederhalskanker
12 september 1995

Wijziging artikel 7 Wet persoonsregistraties
14 juli 1995

Elektronische snelwegen
10 mei 1995

Verstrekken van informatie uit Nationaal Schengen Informatie Systeem aan European Car Register
23 februari 1995

Politieregisters en protocol
december 1994

Herziening adviesstelsel
15 november 1994

Herinrichting Algemene Bijstandswet
26 oktober 1994

Verordening bestrijding EG-fraude
29 september 1994

EG-richtlijn bescherming persoonsgegevens
23 september 1994

Voorontwerp cryptografie
3 mei 1994

Besluit Gemeeentelijke Basisadministratie
23 maart 1994

Nummeridentificatie
25 februari 1994

Wijziging Organisatiewet Sociale Verzekering
26 januari 1994

Wet bevordering evenredige arbeidsdeelname allochtonen
25 november 1993

Wijziging Besluit politieregisters (MOT)
22 november 1993

Gegevensverstrekking van ministerie LNV aan ministerie SZW
16 november 1993

Besluit beheer regionale politie

26 oktober 1993

Wijziging Besluit politieregisters
18 augustus 1993

Wijziging Wet persoonsregistraties inzake heffingen
8 juli 1993

Bestrijding misbruik 06-11
8 juli 1993

Besluit patiëntendossier BOPZ
14 juni 1993

Hoofdlijnennotitie Arrestantenzorg
7 juni 1993

Machtiging Landelijke Organisatie Slachtofferhulp
23 maart 1993

Wijziging Besluit genormeerde vrijstelling
17 februari 1993

Registratie van kentekens
9 december 1992

CID-regeling 1991, modelreglementen CID-register en 'grijze-veld register’
7 december 1992

Politiesamenwerking geautomatiseerde systemen
25 november 1992

Wijziging Wet Bijzondere opnemingen in psychiatrische ziekenhuizen (Wet BOPZ)
19 oktober 1992

Wijziging Besluit registratie justitiële gegevens
12 oktober 1992

Wijziging Besluit ter uitvoering van de Wet arbeid gehandicapte werknemers
5 oktober 1992

Tijdelijke Wet bevordering arbeidsdeelname allochtonen
4 juni 1992

Besluit genormeerde vrijstelling
8 april 1992

Aanpassing Wet op de justitiële documentatie
30 maart 1992

Registratie etniciteit in arbeidsverhoudingen en arbeidsvoorziening
25 februari 1992

Concept-nota Registratie en Rapportage Minderhedenbeleid
3 februari 1992

Regeling vrijstelling protocolplicht (BPOL)
31 januari 1992

Uitvoering van artikel 17, zesde en zevende lid, van het Besluit politieregisters
15 augustus 1991

Uitvoering van artikel 32, tweede lid, van de Wet politieregisters
14 augustus 1991

Machtiging ex artikel 14 lid 1 onder k Besluit politieregisters
31 juli 1991

Wet waardering onroerende zaken (WOZ)
16 juli 1991

Regels inzake documenten dienende ter vaststelling van de identiteit van personen (Wet op de identificatieplicht)
2 juli 1991

Besluit gevoelige gegevens
14 januari 1991

Besluit politieregisters
30 november 1990

Voorontwerp van wet invoering sociaal-fiscaal nummer gemeenten

16 juli 1990

Bijlage 3 Onderzoeksrapporten

[Alle onderzoeksrapporten kunt u aanvragen bij de Registratiekamer. Tekst en/of samenvatting van de meeste onderzoeksrapporten kunt u ook vinden op de website www.registratiekamer.nl]

Onderzoeksrapporten uitgebracht in 1998

Doorzenden reclasseringsrapport
december 1998

Medicatiebewaking
oktober 1998

Beveiliging persoonsgegevens door ministerie
juli 1998

Doorgeven persoonsgegevens door garage-houders aan importeur
juli 1998

Beroepscode psychologen
juli 1998

Openbaar maken van fokgegevens
juli 1998

Gegevenscontrole uit rijksinspectie
juni 1998

Persoonsgebonden clubcard II
mei 1998

Persoonsgebonden clubcard
februari 1998

Onderzoeksrapporten uitgebracht in de periode 1997-1993

Samenwerkingsverbanden en gegevensuitwisseling Werk en Inkomen
10 december 1997

Registratie van prostituées in Groningen
23 december 1997

Nationale Auto Pas (2): registratie van gereden kilometers
juli 1997

Medicatiebewaking door centrale patiëntenregistratie
juli 1997

Registratie van prostituées door politie
16 juni 1997

Privacybescherming in de uitvoering van de Algemene bijstandswet
juni 1997

Persoonsgegevens ter incasso-verstrekking van gegevens uit de GBA aan incassobureaus
maart 1997

In beeld gebracht - Privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging
20 januari 1997

Als de telefoon wordt opgenomen
25 november 1996

Call Centers ECI BV
18 november 1996

Call Centers Postbank NV
18 november 1996

Onderzoek handelsinformatiebureau
augustus 1996

Geheimhouding van persoonsgegevens
juli 1996

Credit Scoring Database

juni 1996

Kredietregistratie BKR
20 juni 1996

Inzage van testgegevens
april 1996

Medisch advies & privacy
14 februari 1996

Afloopberichten in Strafzaken
8 februari 1996

Prijs van een afschrift
25 oktober 1995

Gesloten verstrekkingenregime van de Wet politieregisters
31 juli 1995

Registratie op etniciteit en privacywaarborgen
18 juli 1995

Machtiging tot inzage en correctie
31 maart 1995

Verstrekken van gegevens over een levensverzekeringspolis
17 februari 1995

Verstrekking van persoonsgegevens aan de Vereniging voor de Effectenhandel
16 januari 1995

Inzage van testgegevens
18 oktober 1994

Registratie van bezoekers van "De Schie"
24 oktober 1994

Inzage in dossiers FIOM
12 september 1994

Wet Melding Zeggenschap
25 juli 1994

Reikwijdte artikel 50 OSV
17 juni 1994

Nationale Autopas
23 februari 1994

Rekening van de Arts
11 februari 1994

Incassosysteem GEB
21 januari 1994

Gemeentevervoerbedrijf Amsterdam
12 november 1993

Prostituanten registratie Groningen.
15 oktober 1993

Openbare Bibliotheek Dordrecht
21 september 1993

Debiteurenadministratie in Zandvoort
17 september 1993

Griepvaccinatie
16 september 1993

Verstrekking van de ontslagdiagnosecode
27 augustus 1993

Inrichting van een interkerkelijke ledenadministratie van de SILA
30 juni 1993

Casusregisters in de geestelijke gezondheidszorg
9 juni 1993

Beschikbaarstelling van micro-databestanden van het CBS voor wetenschappelijk onderzoek
26 februari 1993

Reglementen voor politieregisters
februari 1993

Bijlage 4 Achtergrondstudies en Verkenningen

[Alle publicaties in de serie Achtegrondstudie en Verkenningen kunt u aanvragen bij de Registratiekamer. Tekst en/of samenvatting van de meeste publicaties kunt u ook vinden op de website www.registratiekamer.nl]

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 anonimity*. revised edition. A&V-11, Registratiekamer 1998, *f* 25.

Almelo, L. van, e.a., *Gouden bergen van gegevens. Over datawarhousing, 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, ƒ 25.

Overige publicaties

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.

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

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

Proceedings of the 16th International Conference on Data Protection, The Hague 1994 - Facing Dilemmas Registratiekamer 1995, ƒ 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 kunt aanvragen bij de Registratiekamer. Een actueel overzicht vindt u op de website www.registratiekamer.nl]

De Wet persoonsregistraties - de bescherming van uw persoonlijke gegevens, Registratiekamer 1996

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

Registratiekamer, Registratiekamer 1996

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

[De tekst van de Informatiebladen vindt u ook op de website www.registratiekamer.nl]

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*, april/juni/augustus/oktober/december 1998, Sdu Uitgevers, Den Haag 1998

Alonso Blas, D., ‘Las autoridades de control en el campo de la protección de datos personales antes y después de la directiva europea: el ejemplo de Bélgica’ in *Encuentros sobre Informatica y Derecho* 1997-1998, p. 57-70, Universidad Pontificia de Comillas, Madrid, Aranzadi editorial.

Alonso Blas, D., ‘La Protección de Datos en los diferentes Estados que componen la Unión Europea and Estados Unidos’ in Davara Rodriguez, M.A., *La protección de datos en Europa: principios, derechos y procedimiento,* p. 63-187, Universidad Pontificia de Comillas, Grupo Asnef Equifax, Madrid 1998.

Alonso Blas, D., ‘Variations in implementation of the Data Protecion Directive’, *Privacy Laws & Business International Newsletter*, N°45, September 1998.

Alonso Blas, D. en Zeeuw, J. de, ‘Data protection and road-pricing: the use of new technologies for road surveillance’ *Privacy en Informatie*, oktober 1998.

Artz, M.J.T. en Holsheimer, M., ‘Nieuwe wet legt analyse klantgegevens aan banden’ *Automatiseringsgids,* 10 april 1998

Artz, M J.T., e.a. ‘Marketing en de WBP-proef’ *Privacy & Informatie,* december 1998.

Artz, M.J.T., ‘Verwerking van gevoelige gegevens voor marketingdoeleinden’ *Memo Human Inference*, december 1998.

Bogaards, E., ‘Privacybescherming en SJD’ *Tijdschrift voor Sociaal Juridische Dienstverlening*, december 1998

Borking, J.J. en T.F.M. Hooghiemstra, ‘Electronic patient records and hospital information networks’ in: *Health Information Initiatives in The Netherlands*, april 1998.

Crouwers, B. ‘Respect voor privacy in dataming loont’ *ITEMS*, november 1998

Eck, B.M.A., ‘Over camerabewaking en privacy’ in Beerepoot, A.F.J. e.a. (red.), *Beveiligingsjaarboek 1998*, Noorduin, Deventer: 1998

Eck, B.M.A., ‘SWI en privacy’, *Nieuwsbrief Service centra van de overheid*, maart 1998

Hooghiemstra, T.F.M., ‘De WBP en de gezondheidszorg’ *Nederlands Tijdschrift voor de Medische Administratie*

Hooghiemstra, T.F.M., ‘Privacy op de kinderafdeling’ *Tijdschrift Kinderverpleegkunde* december 1998

Hooghiemstra, T.F.M., ‘De WBP en de gezondheidszorg’ *Nederlands Tijdschrift voor de Medische administratie*, september 1998.

Pol, U. van de, ‘Geen privacybescherming zonder publiciteit’ *Mediaforum* 1998

Pol, U. van de, ‘De rol en sanctiebeleid van de Registratiekamer’ *Privacy & Informatie*, april 1998

Pol, U. van de, ‘Een bloemlezing over personeelsvolgsystemen’ in *De werknemer achtervolgd?! Over personeelsvolgsystemen, verzuimcontrole en de nieuwe bevoegdheden van de OR*, Sinzheimer Cahiers 14, SDU, Den Haag 1998.

Stratum, M. van, ‘Vraagtekens’, *Algemeen Politieblad*, 7 november 1998

Terstegge, J.H.J., ‘Enkele opmerkingen naar aanleiding van Centrale Raad van Beroep 25 februari 1998’, nr.96/7142 (JB 1998/61), *Jurisprudentie Bestuursrecht*, 5, 23 april 1998

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

Terstegge, J.H.J., ‘Medische keuringen, ziekteverzuim en privacy’, in: J.H.J. Terstegge en H.H. de Vries (red.): *De werknemer achtervolgd?*, Sinzheimer Cahiers 14, SDU, Den Haag 1998

Vries, H.H. de, ‘Verborgen camerabewaking’, *Privacy & Informatie*, april 1998

Vries, H.H. de, ‘Pemba en art. 6 EVRM’, *Privacy & Informatie*, augustus 1998

Vries, H.H. de, ‘Bewijs op videoband’, *Privacy & Informatie*, augustus 1998

Vries, H.H. de, ‘Privacyrevolutie in de polder’, *Sociaal Recht*, 10, 1998

Vries, H.H. de met T. Weijers, *Zicht op telewerken*, VUGA, november 1998

Vries, H.H. de, ‘De nieuwe bevoegdheden van de ondernemingsraad’, in: J.H.J. Terstegge en H.H. de Vries (red.): *De werknemer achtervolgd?*, Sinzheimer Cahiers 14, SDU, Den Haag 1998

Vries, H.H. de, met U. van de Pol, ‘Checklist voor de OR’, in: J.H.J. Terstegge en H.H. de Vries (red.): *De werknemer achtervolgd?*, Sinzheimer Cahiers 14, SDU, Den Haag 1998

Vries, H.H. de, met A. Holleman, S. Nouwt en E. Vunderink, ‘Commentaar voorstel WBP’, in: A. Holleman (red.) *Handboek Privacybescherming*, Samsom (losbladig)

Vries, H.H. de, ‘De OR en de privacy van werknemers’, *Sociaal Beleid*, Samsom, december 1998.

Vries, H.H. de, ‘Noot bij CRvB 27 november 1998’, *Uitspraken Sociale Zekerheid*, december 1998

Bijlage 7 Gedragscodes

Gedragscodes waarvoor de Registratiekamer een Verklaring van Overeenstemming heeft verleend

Gedragscode verwerking persoonsgegevens verzekeringsbedrijf (Verbond van Verzekeraars), geldig tot 5 maart 2001 (Strct. 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)
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)
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)
Herkenningsdienst (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)
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 Herkenningsdienst (Stcrt. 1996,125)
Openbare orde taken Regionale Inlichtingendiensten (Stcrt. 1996,125)
Bureau Financiële Ondersteuning (Stcrt. 1996,125)

Bijlage 9 Formatie 1995-1998

Formatie per 31 december uitgedrukt in volledige arbeidsplaatsen (fte)

	1995	**1996**	**1997**	**1998**
beschikbaar	39,4	39,4	41,4	43
bezet	38	37,9	37,8	41.5
aantal medewerkers	42	42	43	47

Bijlage 10 Activiteiten 1995-1998 in cijfers

	1995	**1996**	**1997**	**1998**
Adviezen aan regering en parlement	15	18	27	18
Onderzoeksrapporten	6	10	7	9
Achtergrondstudies en Verkenningen	5	1		6
Overige publicaties	1	1	1	1
Klachten en geschillen	209	245	374	319
Schriftelijken verzoek om advies	313	328	517	595
Telefonisch spreekuur	3520	4720	4970	5500
Aanmeldingen	53629	55601	57786	61111

Colophon

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

samenstelling & eindredactie: Diana Alonso Blas & Bart Crouwers

Met bijzondere dank aan: Hester de Vries, Bernard Hulsman, Ronald Hes, Marlies van Eck, Erik Bogaards, Carine Zandee, Guus de Heij en Mirjam Hazenoot.