Jaarverslag 2000

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

ISBN 90 74087 28 0
mei 2001

Registratiekamer

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

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

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

Ten geleide

Er is onderzoek ingesteld naar de houding van consumenten tegenover privacy op internet in elf Europese landen en Zuid-Afrika (PricewaterhouseCoopers, *E-privacy: Het dichten van de kloof tussen Business en Consumers).* Twee conclusies uit dat onderzoek zijn:

- Consumenten maken zich werkelijk zorgen over de gevaren voor hun privacy on line. Privacykwesties zijn daarom bepalend voor zowel de mate waarin consumenten bepaalde transacties afsluiten als de aard van die transacties.
- Consumenten stellen intuïtief meer vertrouwen in technologie dan in regels of wetgeving. Biedt daarom een reeks oplossingen aan die alle terreinen omvat, waaronder de technische en juridische aspecten.

Deze uitkomsten ondersteunen de Registratiekamer in het werken volgens het viersporenbeleid. Dat omvat immers, naast bewustwording en handhaving, ook technologie en normontwikkeling.

Hoe is dit jaarverslag opgebouwd? In hoofdstuk 1 wordt in vogelvlucht een impressie gegeven van de activiteiten van de Registratiekamer in 2000. In de hoofdstukken 2, 3 en 4 vindt u een bespreking van drie thema's die in 2000 centraal stonden en waarvan verwacht mag worden dat ze ook de komende jaren nog volop in de belangstelling zullen staan. De reguliere activiteiten van de Registratiekamer zijn op hoofdlijnen weergegeven in hoofdstuk 5, volgens een indeling die parallel loopt met het ontwikkelde 'viersporenbeleid'. Hoofdstuk 6 gaat in op de veranderingen die de organisatie in 2000 heeft doorgemaakt. Het jaarverslag van de Registratiekamer kent een nieuw hoofdstuk, de Vooruitblik. Hierin worden de speerpunten van 2001 toegelicht. Het geeft weer waar onze speerpunten liggen. In een volgend jaarverslag wordt dit hoofdstuk aangevuld met een terugblik. Het geeft dan ook aan wat er van de voorgestelde speerpunten is gerealiseerd. Overzichten van aangemelde persoonsregistraties, uitgebrachte adviezen, onderzoeksrapporten en achtergrondstudies, gepubliceerde artikelen en overige gegevens, vindt u in de bijlagen. De aangemelde persoonsregistraties worden minder gedetailleerd weergegeven dan voorgaande jaren. De volledige lijst is beschikbaar op de internetsite van de Registratiekamer.

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

Wilt u naar aanleiding van dit jaarverslag op de hoogte blijven van de voortgang van de nieuwe wet, de activiteiten of de publicaties van de Registratiekamer? Dan kunt u putten uit diverse andere bronnen met informatie: het katern 'Berichten van de Registratiekamer' in het tijdschrift *Privacy & Informatie*, de uitsprakenbundel *Persoonsgegevens beschermd* en de internetsite van de Registratiekamer: www.registratiekamer.nl, vanaf 1 september 2001: www.cbpweb.nl.

mr. P.J. Hustinx (voorzitter)

drs. J.J. Borking (lid)

dr. U. van de Pol (lid)

Inhoud

In vogelvlucht 2000

2000 in vogelvlucht

Er zijn drie ontwikkelingen in de informatiemaatschappij die in verband met de persoonlijke levenssfeer de aandacht vragen. Allereerst zijn de technologische mogelijkheden waarmee gegevens verzameld, vastgelegd, gekoppeld, geordend, bewerkt en geanalyseerd – kortom verwerkt – worden, de laatste jaren sterk toegenomen. Zowel de inhoud als het patroon van de communicatie op internet en via mobiele telefonie kunnen bijvoorbeeld op eenvoudige wijze worden vastgelegd. Ook de vooruitgang in het DNA-onderzoek creëert steeds meer mogelijkheden om gegevens van personen te verkrijgen en te gebruiken voor uiteenlopende doeleinden. Dit leidt ertoe dat organisaties of personen, zoals overheidsinstellingen, bedrijven of werkgevers, steeds meer greep op persoonsgegevens krijgen.

Tegelijkertijd zien we de ontwikkeling om aan de burger of klant maatwerk te leveren bij het aanbieden van diensten en producten. De één-op-één benadering van de klant wordt steeds populairder. Het bedrijfsleven heeft voor deze gerichte benadering behoefte aan profilering van de klant. Deze direct-marketingtechniek breidt zich uit naar andere sectoren in de maatschappij: zorgverzekeraars willen steeds vaker over de schouder van arts en apotheker meekijken om inzicht te krijgen in de behoeften van patiënten en de overheid wil haar toegankelijkheid voor de burger vergroten en benadert hierbij de burger pro-actief. Dat lukt alleen als de overheid de communicatie met en óver de burger kan stroomlijnen. Het gevolg is dat de overheid de burger beter leert kennen.

In het kader van de verdergaande efficiency bij de overheid is tot slot de ontwikkeling waarneembaar van vervagende grenzen tussen het publieke en private domein. Zo werkt de politie steeds vaker samen met ambtenaren van controlerende diensten of functionarissen uit de gezondheidszorg, de maatschappelijke dienstverlening of het bedrijfsleven. Een ander voorbeeld: in het kader van de herstructurering van de sociale zekerheid worden private partijen betrokken bij het begeleiden van uitkeringsgerechtigden naar de arbeidsmarkt en wisselen betrokken partijen veelvuldig gegevens uit.

Deze ontwikkelingen hebben ertoe geleid dat bestanden gekoppeld worden in datawarehouses en er meer gegevensstromen ontstaan tussen instanties. Tevens is sprake van een toename van de kring van organisaties die gegevens met elkaar uitwisselen. De behoefte aan basisadministraties groeit en is bijvoorbeeld zichtbaar in het onderwijs en de sociale zekerheid. Bovendien wordt steeds meer datamining gebruikt, waardoor tot dan toe onbekende patronen over mensen uit databanken kunnen worden gedestilleerd.

Informatieplicht aangescherpt

De bescherming van de persoonlijke levenssfeer kan door de bovenstaande drie ontwikkelingen in de knel komen. De vele mogelijkheden om persoonsgegevens buiten medeweten van de geregistreerde te verwerken zijn immers evenzovele bedreigingen van de persoonlijke levenssfeer in de informatiemaatschappij. Zo zijn internetserviceproviders over het algemeen niet helder over de informatie die gebruikers verplicht moeten of vrijwillig kunnen afstaan en over het gebruik van informatie over het surfgedrag. Het bank- en verzekeringswezen, dat klanten steeds meer een totaalpakket van financiële producten aanbiedt, hanteert vaak een ruime doelomschrijving voor de verwerking van persoonsgegevens. In beide gevallen geldt dat dit dan onvoldoende houvast biedt om concrete verwerkingen van persoonsgegevens op hun rechtmatigheid te kunnen toetsen, en dit biedt in het algemeen onvoldoende inzicht in deze processen. In concrete situaties is specificatie van de doelomschrijving vereist.

Bij het aangaan van samenwerkingsverbanden tussen zowel publieke instanties onderling als tussen publieke en private partijen is de informatiehuishouding en de onderlinge informatie-uitwisseling vaak niet duidelijk omschreven en bovendien niet wettelijk geregeld: zo wordt er in het kader van de opsporingstaak van politie en justitie vaak gewerkt op basis van – moeilijk controleerbare – vrijwillige medewerking. De Registratiekamer heeft als standpunt dat de hoofdlijnen van de gegevensverwerking bij dergelijke samenwerkingsverbanden in formele wetgeving moeten worden vastgelegd.

Om tegenwicht te bieden tegen de geschetste ontwikkelingen is de informatieplicht in de Wet bescherming persoonsgegevens (WBP) aangescherpt. Voor de geregistreerde (in de terminologie van de WBP de betrokkene) moet het immers helder zijn wat er met zijn gegevens gebeurt. Hij moet worden geïnformeerd over het verwerken van zijn gegevens, over het doel van deze verwerking en weten wie daar de verantwoordelijke voor is. Alleen dan kan hij zijn rechten, zoals het recht op inzage en correctie, daadwerkelijk uitoefenen.

Doelbinding

Dankzij nieuwe technologieën kunnen gegevens gemakkelijk vastgelegd en verder gebruikt worden. Het wordt steeds eenvoudiger gegevens tussen organisaties uit te wisselen. De doelbinding kan hierdoor onder druk komen te staan. Het beginsel van de doelbinding betekent dat het doel waarvoor persoonsgegevens worden verzameld of verkregen, bepalend is voor het verdere gebruik van deze gegevens. Met andere woorden: het verdere gebruik dient verenigbaar te zijn met het oorspronkelijke doel van de verwerking. Relevante factoren om de verenigbaarheid van het verdere gebruik te toetsen zijn met name of het oorspronkelijke en nieuwe doel verwant zijn, of het gaat om gevoelige of vertrouwelijke gegevens, of de gegevens vrijwillig of verplicht zijn verstrekt, of er beslissingen genomen worden die gevolgen hebben voor de betrokken personen en of de betrokken personen hierover geïnformeerd zijn. Ook is van belang of het nieuwe doel ook op minder ingrijpende wijze kan worden bereikt. Toezicht hierop, met name door middel van audits, is een onmisbaar sluitstuk.

De trend van maatwerk in dienstverlening en de (deels daarmee gepaard gaande) verdergaande publiek-private samenwerking leiden tot verdere verwerking van gegevens. Vooral bij publiek-private samenwerking kan dit problematisch zijn omdat de verwerkingsgronden, de wijze van verkrijging en de doelstellingen in deze sectoren doorgaans van elkaar verschillen. Een belangrijk aandachtspunt is op welke wijze een zorgvuldige omgang met persoonsgegevens bij samenwerking en bij het overdragen van overheidstaken naar private instanties gewaarborgd kan blijven. Een gescheiden informatiehuishouding voor verschillende doelen is hierbij van belang.

Het verdere gebruik van persoonsgegevens in andere dan de oorspronkelijke sector en voor nieuwe doelen neemt een vlucht. Zo is er de wens strafrechtelijke gegevens aan derden buiten de strafrechtsketen te verstrekken en wordt het sofi-nummer gebruikt door de politie voor het vaststellen van iemands identiteit en door private partijen bij de uitvoering van de nieuwe sociale zekerheidswetgeving. Het zal tevens ingevoerd worden in het onderwijs ter bestrijding van fraude door instellingen. Ook is er behoefte aan verder gebruik van DNA-materiaal. Telkenmale zal moeten worden afgewogen of de verdere verwerking van deze gegevens daadwerkelijk noodzakelijk is.

Terughoudendheid is gewenst bij de uitwaaiering van unieke persoonsgegevens, zeker in een tijd van verdergaande automatisering. Niet het instrument van unieke persoonsgegevens als zodanig behoeft tot onaanvaardbare gevolgen te

leiden. Problemen kunnen ontstaan doordat het faciliterende karakter steeds weer nieuwe gebruiksmogelijkheden genereert. Het opzetten van basisregistraties of centrale registers behoort tot de mogelijkheden. Er kan zo een uniek persoonsnummer of persoonsprofiel voor algemeen gebruik ontstaan. De Registratiekamer blijft een sterke voorkeur houden voor sectorspecifieke persoonsnummers of andere persoonsgegevens. Als toch wordt besloten unieke persoonsgegevens in bredere kring en voor meerdere doelen te gebruiken zijn naast een adequate wettelijke grondslag expliciet beperkende gebruiksbepalingen noodzakelijk om aan het verenigbaarheidsvereiste te voldoen.

Naast de aangescherpte informatieplicht en de doelbinding kan ook technologie bijdragen aan het bevorderen van een privacyveilige omgeving. De nieuwe wet biedt dan ook goede mogelijkheden om privacybescherming op te nemen in de inrichting van informatiesystemen en netwerken. Zo wordt technologie niet langer als een bedreiging voor de privacy beschouwd, maar kan deze juist een oplossing bieden voor privacyproblemen.

Thema's

Steeds meer worden we in beeld gebracht. Al in 1997 stelde de Registratiekamer hiervoor regels op. De impact van cameratoezicht wordt versterkt doordat de systemen steeds intelligenter worden. In centrale meldkamers kan heel Nederland vanaf één plek in de gaten worden gehouden. De zegen van meer veiligheid krijgt dan ook een keerzijde: een veelomvattend volgsysteem is immers een geweldige inbreuk op de privacy van de burger (zie thema 1).

In de gezondheidszorg gaan veel gegevens om. Dat is niet alleen nodig voor de zorg aan patiënten, maar ook voor de financiering, voor onderzoek en voor beleidsontwikkeling. Oprukkende informatietechnologie kan op gespannen voet komen te staan met privacywaarborgen. Denkt men in de zorg wel voldoende na over de bescherming van persoonsgegevens (zie thema 2)?

De privacy van de burger kan in drie rollen op internet geschaad worden. Zijn privacy is in het geding als hij toegang wil tot het net (hoe gaat een provider om met zijn persoonsgegevens?), als hij als werknemer te maken krijgt met controle op zijn e-mail- en internetgebruik door zijn werkgever en als hij door politie en justitie als verdachte van cybercrime wordt gezien. In het derde thema worden de dilemma's geschetst en verslag gedaan van internationaal onderzoek naar privacy en internet.

Belangrijkste publicaties

De Registratiekamer is onder meer belast met het toezicht op de naleving van de Wet politieregisters (Wpolr) en de daarbij behorende uitvoeringsregelingen. Zij rekent de ontsluiting van deze wetgeving mede tot haar taak. Daarom heeft zij aan ITS en de Katholieke Universiteit Brabant verzocht om haar rapport *Het gesloten verstrekkingenregime van de Wet politieregisters* uit 1995 te actualiseren en te bewerken. De bewerking heeft bijgedragen aan een vergroting van de toegankelijkheid van de voor deze wetgeving relevante uitspraken en ontwikkelingen. De bewerking verscheen onder de titel *Politiegegevens beschermd – Een toelichting op het gesloten verstrekkingensysteem van de Wet politieregisters*.

De vraag naar het rapport *Privacy-Enhancing Technologies: the path to anonimity* was zo groot dat besloten werd tot een herdruk.

Indicatiestelling is een belangrijk instrument in de gezondheidszorg. De zorgvrager zal zorg op maat willen krijgen van de zorgverlener en de

verzekeraar zal willen beoordelen of de zorgvrager aanspraak kan maken op de zorg die hij zegt nodig te hebben. In deze benadering wordt de verzekeraar als zorgtoewijzer nauw betrokken bij het stellen van indicaties. In het rapport *Zorg voor gegevens bij indicatiestelling – Aanbevelingen voor de praktijk van indicatiestelling* worden de mogelijkheden en grenzen aangegeven van het verkrijgen/verzamelen, vastleggen en gebruiken, uitwisselen en bewaren van de gegevens bij de praktijk van indicatiestelling. De Registratiekamer hoopt met dit rapport en de aanbevelingen een handreiking te bieden die met name vanuit het oogpunt van de privacybescherming een verantwoorde indicatiestelling, rechtmatigheidstoetsing, wachtlijstbeheer en zorgtoewijzing mogelijk maakt.

De Registratiekamer heeft onderzocht op welke wijze internetproviders persoonsgegevens verzamelen en verder gebruiken. Hierbij is betrokken de wijze waarop klanten worden geïnformeerd over het gebruik van hun gegevens. Uit de publicatie *Klant in het Web* is de belangrijkste conclusie dat de bescherming van gegevens door internetproviders tekort schiet.

Een bedrijf moet winstgevend zijn om te kunnen overleven. Een bedrijf dat producten op krediet levert, wil daarom alleen 'goede' klanten aan zich binden. Goede klanten zijn o.a. die klanten die hun rekeningen betalen. Een techniek om het betalingsgedrag te voorspellen is 'credit scoring'. Een score wordt vaak in een getal uitgedrukt. Als een klant onder een bepaalde waarde scoort, wordt deze klant niet (meteen) geaccepteerd. In de studie *De gewaardeerde klant* ligt de nadruk op kredietbeoordelingen waarbij derden zijn betrokken zoals informatiebureaus.

Etnische afkomst is een factor die het consumptiepatroon beïnvloedt. Bedrijven proberen daarom steeds gerichter allochtone bevolkingsgroepen te interesseren voor hun producten. Het registreren van mensen van een bepaalde etnische afkomst kan een middel zijn om bepaalde groepen te bereiken. Wanneer etniciteit geregistreerd wordt ontstaat echter ook de mogelijkheid om mensen uit te sluiten op grond van hun etnische afkomst. Over deze problematiek verscheen *Herkomst van de klant*.

De vooronderstelde verstrengeling van diensten en producten bij financiële conglomeraten is minder ver gevorderd dan was verwacht. Ook de technologische mogelijkheden van integratie van de ICT-infrastructuur zijn minder ver dan verwacht. Het gaat veelal om plannen. Dit zijn de voornaamste conclusies uit het onderzoek naar gegevensverwerking in financiële conglomeraten *(Bankverzekeraars en privacy)*. De Registratiekamer heeft dit onderzoek uitgevoerd om inzicht te verkrijgen in hoe binnen deze conglomeraten feitelijk wordt omgegaan met persoonsgegevens en hoe de bescherming van de persoonlijke levenssfeer in de praktijk is vormgegeven.

Elektronische controle van computergebruik roept vragen op over de bescherming van de persoonlijke levenssfeer van de werknemer. Een groot aantal werkgevers, ondernemingsraden en individuele werknemers heeft deze vragen voorgelegd aan de Registratiekamer, die daarop een studie heeft verricht naar de controle op e-mail- en internetgebruik. Dit heeft geresulteerd in het rapport *Goed werken in netwerken*.

Actief op internationaal gebied

Internationaal bezien is de artikel 29 Werkgroep van de Europese privacyrichtlijn van belang. In deze werkgroep hebben alle Europese toezichthoudende autoriteiten zitting. De werkgroep heeft in het verslagjaar in

het bijzonder aandacht besteed aan de problematiek rond het verkeer van persoonsgegevens naar landen buiten de Europese Unie. De werkgroep adviseerde de Europese Commissie over het zogenoemde 'safe harbor' arrangement voor Amerikaanse bedrijven. Hierdoor is gegevensuitwisseling met bedrijven in Amerika mogelijk, indien deze bedrijven zich zullen houden aan de principes en voorwaarden die in het safe harbor arrangement vastgesteld zijn. Bedrijven die meedoen, worden gezien als bedrijven met een adequaat beschermingsniveau in de zin van de richtlijn.

De Registratiekamer heeft bijgedragen aan activiteiten van drie subgroepen van de artikel 29 Werkgroep: de Internet Task Force, de subgroep die zich bezighoudt met de beoordeling van communautaire gedragscodes, en de subgroep voor contractuele bepalingen die gebruikt zouden kunnen worden voor de internationale uitwisseling van gegevens. Een beslissing van de Europese Commissie over modelcontracten wordt in 2001 verwacht.

Landen buiten de Europese Unie tonen grote belangstelling voor de Europese privacywetgeving. Landen die in de toekomst lid willen worden van de Europese Unie, proberen regels te ontwikkelen die voldoen aan de eisen van zowel het dataprotectieverdrag van de Raad van Europa als de Europese richtlijn. Op verzoek van de Europese Commissie en de Raad van Europa heeft de Registratiekamer deelgenomen aan twee missies naar Bulgarije en Polen. Zij heeft verder informatiesessies georganiseerd voor bezoekers uit Japan, Rusland, Hong Kong, de Verenigde Staten, Moldavië, Zwitserland en de Tsjechische Republiek. Op verzoek van de Consumentenbond is een seminar gehouden voor leden van Consumers International, het internationale samenwerkingsverband van consumentenbonden.

De Registratiekamer vertegenwoordigt Nederland ook in de adviescommissie van het dataprotectieverdrag van de Raad van Europa. De commissie heeft de tekst van een protocol voor het dataprotectieverdrag vastgesteld. In dit protocol worden twee onderwerpen behandeld: de derde-landenproblematiek en de rol van de toezichthoudende autoriteiten. De tekst van dit protocol kan geraadpleegd worden op de website van de Raad van Europa: www.coe.fr

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

Samenwerking met andere toezichthoudende autoriteiten speelt een cruciale rol in het kader van de Europese privacyregels. Tijdens de lenteconferentie van Europese toezichthoudende autoriteiten in Stockholm heeft de Registratiekamer een rapport over audittechnieken gepresenteerd aan de Europese zusterinstellingen. Dit rapport werd opgesteld in samenwerking met de Spaanse Agencia de Protección de Datos.

Op initiatief van de Registratiekamer en haar Engelse zusterorganisatie is in 2000 een serie workshops voor medewerkers van toezichthoudende autoriteiten gestart over praktische onderwerpen, zoals de behandeling van klachten met internationale aspecten. Na een eerste workshop in Manchester, heeft de Registratiekamer een tweede workshop georganiseerd. Medewerkers van vijftien Europese toezichthoudende autoriteiten en van de Europese Commissie hebben actief deelgenomen aan deze informele bijeenkomst.

thema

Bezinning op videocameratoezicht

Het gebruik van videocamera's voor het uitoefenen van toezicht in openbare ruimten komt in een stroomversnelling met alle risico's van dien. Er hangen camera's boven de snelwegen, in het openbaar vervoer (tram, bus of metro) en op de NS-stations. Ben je eenmaal in het centrum dan zijn er bewakingscamera's in winkels, banken en tal van andere openbare ruimtes.

Gericht cameragebruik kan – ook in de ogen van de Registratiekamer – een waardevol onderdeel zijn van een breder pakket aan veiligheidsmaatregelen. Ongebreideld gebruik dient echter geen zinnig doel en vormt daarmee een ongerechtvaardigde aantasting van de privacy van de burgers. Maathouden is daarom noodzakelijk. Even cruciaal is het dat de overheid de regie blijft voeren in het publieke domein. Het belang van deze uitgangspunten wordt onderstreept door de technische ontwikkelingen. Verfijnde detectiesystemen kunnen ongewenst gedrag en gezochte burgers opsporen. Centrale meldkamers vergroten de slagvaardigheid van camerasystemen.

Gelet op deze dynamische groei van cameratoezicht, naar omvang en intensiteit, roept de Registratiekamer op tot bezinning op de inzet van cameratoezicht in het publieke domein. De burgers moet – zeker als het om zijn veiligheid gaat – wel gezien, maar niet constant bekeken worden.

Opstellen van regels

Steeds meer wordt de burger "in beeld gebracht". Onder deze titel bracht de Registratiekamer al in 1997 privacyregels uit voor het gebruik van videocamera's voor toezicht en beveiliging. Zij bespeurde namelijk een groeiende tendens naar het gebruik van deze vorm van toezicht. Als op winkelpleinen, in uitgaanscentra en in (semi) openbare gebouwen de burger zich niet langer veilig voelt, als beveiliging en bewaking op de traditionele wijze niet meer voldoen of erg kostbaar worden, bieden videocamera's kennelijk een uitkomst. Steeds vaker wordt overgegaan tot de installatie van geavanceerde videobewakingssystemen om het gedrag van het publiek in het oog te houden.

Omdat cameratoezicht op gespannen voet kan komen met de bescherming van privacy van de aanwezige personen, achtte de Registratiekamer het van groot belang dat duidelijk is wanneer en onder welke voorwaarden dit middel gerechtvaardigd is. Op basis van bestaande wetgeving en Europese verdragen stelde de Registratiekamer daarom een aantal regels op voor het gebruik van videosystemen voor toezicht en beveiliging.

In veel gemeenten zijn inmiddels op meer of minder grote schaal videocamera's in gebruik, vaak in samenwerking met de plaatselijke politie. Ook een groeiende aantal bedrijven exploiteert voor de veiligheid van klant en personeel camerasystemen. Ook is sprake van intensieve samenwerking tussen gemeenten, politie en bedrijven. Zolang de regels van de Registratiekamer gevolgd worden, blijft de inbreuk op de persoonlijke levenssfeer beperkt.

De Registratiekamer stond gelukkig niet alleen in het reguleren van cameratoezicht. Het kabinet reageerde in de herfst van 1997 met een nota waarin de hoofdlijnen van het rapport van de Registratiekamer werden gevolgd en waarin wetgeving werd aangekondigd.

Op 13 oktober 2000 werd de *Handreiking cameratoezicht* gepubliceerd. Deze is bedoeld om de gemeenten informatie te geven bij "wat er allemaal komt kijken bij cameratoezicht", aldus het voorwoord. Een wijziging van het Wetboek van

Strafrecht is ingediend bij de Tweede Kamer. Hierbij wordt de strafbaarstelling van het maken van heimelijke opnamen van personen in artikel 441b van het Wetboek van Strafrecht uitgebreid. Voorgesteld is dit verbod uit te breiden van winkels en horecagelegenheden naar alle voor het publiek toegankelijke plaatsen. In voorbereiding is een wetsvoorstel tot wijziging van de Gemeentewet. Het gaat hierbij om de invoering van regels voor het gebruik van camera's voor toezicht op openbare plaatsen.

Grondrecht in het geding?

Van oudsher kent iedere burger op de openbare weg en in openbare ruimten een zekere mate van privacy die wordt bepaald door de daar heersende betrekkelijke anonimiteit. Iemand is slechts een voorbijganger, te voet of in een auto, een klant of een toevallige bezoeker. Ook al beweegt een burger zich in het openbaar, het onvoorspelbare, het incidentele karakter en het feit dat hij vaak deel uitmaakt van een grotere groep of zelfs opgaat in een massa, zorgen er in het algemeen voor dat iemand wel gezien kan worden maar toch weinig sporen achterlaat.

De groeiende praktijk van het in beeld brengen van burgers brengt daarin verandering. Zonder dat zij daarover zelf enige zeggenschap hebben, worden beelden van mensen vastgelegd. Hiermee wordt hun aanwezigheid, al of niet in gezelschap, op een bepaalde locatie en tijd, in een bepaalde houding en kleding vastgelegd. Het is niet zo dat elke opname die van iemand wordt gemaakt, meteen maar als een privacyschending moet worden aangemerkt. Dat hangt er namelijk ook vanaf in welke situatie, door welke instantie en met welk doel de opnamen worden gemaakt. Maar het is begrijpelijk en in een aantal situaties ook wel terecht dat dit als een inbreuk op de persoonlijke levenssfeer wordt ervaren. Dit betekent nog niet dat deze inbreuk daarmee onrechtmatig is, maar wel zijn grondrechten in het geding. Bescherming tegen onterechte inbreuken en normering van dit gebruik is geboden.

De juridische grondslag is vervat in internationale verdragen en in onze Grondwet. Zo kent artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) ieder het recht op respect voor zijn privé-leven toe. De precieze reikwijdte van dit recht is in de jurisprudentie van het Europese Hof nog niet bepaald. Vereist is echter dat de beperking van dit recht door de overheid in een wettelijke regeling is voorzien.

Verder is vereist dat de beperking noodzakelijk is in een democratische samenleving met het oog op (één van de) in artikel 8, tweede lid, bedoelde belangen. De beperking dient gerechtvaardigd te worden door een dringende maatschappelijke behoefte. Nodig is ook dat de beperking voldoet aan de eisen van proportionaliteit en subsidiariteit: met andere woorden de beperking moet in een juiste verhouding staan tot het nagestreefde doel en het doel moet niet op een minder ingrijpende wijze kunnen worden bereikt. Het Europees Dataverdrag bevat deze en ook meer specifieke uitgangspunten voor de bescherming van het gebruik van gegevens over individuele personen. Het gaat hierbij met name om het belang van de kenbaarheid van het vastleggen van informatie over personen en het begrenzen van het verdere gebruik ervan.

De eerbiediging van de persoonlijke levenssfeer is ook in artikel 10 van de Grondwet verankerd. Voor het maken van een uitzondering daarop gelden niet alleen de genoemde beginselen, maar is ook een grondslag nodig in een formele wet, dat wil zeggen een regeling die door regering en parlement is gemaakt. In het tweede lid van dit artikel is aangegeven dat er regels moeten worden

opgesteld ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Deze regels zijn in de Wet persoonregistraties (WPR) en in de - toekomstige - Wet bescherming persoonsgegevens (WBP) vastgelegd.

Videocameratoezicht in openbare ruimten kan onder omstandigheden een inbreuk vormen op het privé-leven van degenen die in beeld worden gebracht. Deze inbreuk moet dan voldoen aan de hiervoor genoemde eisen. Van de omgang met de door middel van het toezicht verzamelde beelden geldt de wetgeving ter bescherming van persoonsgegevens.

Persoonsgegevens in het geding?

De WPR en de WBP dienen de bescherming van persoonsgegevens. En bij het maken van video-opnamen gaat het veelal om persoonsgegevens. Een video-opname van een persoon die daarop duidelijk is afgebeeld, heeft altijd op hem betrekking en verschaft bovendien informatie over deze persoon, waar iemand was, wat voor kleur haar deze persoon heeft, hoe iemand zich gedraagt. De conclusie is dan ook dat redelijk goede beelden waarop individuen zijn te herkennen als persoonsgegevens kunnen worden aangemerkt. De groeiende digitale verwerking van beeld- en geluidsmateriaal maakt het traceren van personen ook steeds eenvoudiger. Daarom staat dan ook terecht in de memorie van toelichting op de WBP dat een digitale databank met beeltenissen en stemafdrukken onder de werking van deze wet valt (Kamerstukken II, 1997-1998, 25 892 nr. 3, blz. 71).

Inmiddels is ook in de rechtspraak discussie ontstaan over de toelaatbaarheid van het gebruiken van video-opnamen voor de bewijsvoering in strafzaken. Twee op het oog tegengestelde uitspraken hebben de rechtbanken in Dordrecht en Rotterdam gedaan.

De rechtbank Dordrecht beoordeelde het cameragebruik door een ondernemer op zijn recreatieterrein om vandalisme te bestrijden, De rechtbank oordeelde op 30 oktober 2000 dat een dergelijk door een burger ingesteld toezicht een onrechtmatige inbreuk vormde op artikel 8 van het EVRM. De videobanden die als bewijs in een strafzaak werden ingebracht, mochten dan ook niet voor het bewijs van het strafbare feit worden gebruikt.

De rechtbank Rotterdam beoordeelde op 29 augustus 2000 het cameratoezicht door de overheid in een woonwijk. Zij kwam tot het oordeel dat het cameratoezicht weliswaar enige inbreuk vormde op artikel 8 van het EVRM, maar dat deze inmenging van het openbaar gezag was toegestaan. Deze werd gebaseerd op het algemene taakstellende artikel 2 van de Politiewet. Het hoger beroep in deze zaak is nog lopend.

Belangrijke vragen

Bij het opzetten en in gebruik nemen van videocamerasystemen vergt een aantal vragen een bevredigend antwoord.

- Is er een goede reden?
- Op grond van welke bevoegdheid wordt geopereerd?
- Welk doel wordt nagestreefd?
- Wie voert de regie?
- Is er samenhang met andere maatregelen?
- Wordt het bekend gemaakt?
- Wordt maat gehouden?

Is er een goede reden?

Incidenten kunnen de aanleiding voor een gemeente zijn om een discussie over de invoering van cameratoezicht te voeren. Een incident vormt echter nog geen toereikende rechtvaardiging. Zo was de dood van Meindert Tjoelker voor de gemeenteraad in Leeuwarden een goede aanleiding om over de veiligheid op straat te gaan nadenken. Een integraal veiligheidsbeleid werd opgezet. Een publiek debat over de invoering van cameratoezicht met deelname van de Registratiekamer is in 2000 gevoerd. De uitkomst van het debat was dat er op dat moment geen behoefte was aan het invoeren van cameratoezicht.

In Groningen kwam de gemeenteraad tot een andere conclusie. Het uitgaansgeweld was in de binnenstad weliswaar gestabiliseerd, maar de omvang van het aantal delicten was toch zodanig dat betere bestrijding nodig was. De Registratiekamer toetste op verzoek van de burgmeester de Groningse aanpak en beoordeelde deze als evenwichtig. Het in begin 2000 ophangen van camera's op de Grote Markt en het nabijgelegen uitgaanscentrum vormde dan ook een element van het 'veilig uitgaan' in de binnenstad dat onmisbaar kon worden geacht als onderdeel van het integrale veiligheidsplan. Bij de installatie van het systeem begin 2000 riep de Registratiekamer onder meer op tot regelmatige bezinning op het voortgaand gebruik van het systeem.

Ook met de invoering van cameratoezicht in de Haagse prostitutiewijk had de Registratiekamer in 2000 bemoeienis. Het ging hier om het uitoefenen van toezicht op de raamprostitutie. Al eerder adviseerde de Registratiekamer over dergelijke projecten op de Amsterdamse Walletjes en de Alkmaarse Achterdam. Het delicate karakter van deze bedrijfstak vergt steeds een gerichte inzet van camera's. Een overmaat aan toezicht kan – juist vanwege de daaraan inherente inbreuk op de privacy – nadelig zijn voor deze bedrijfstak. Dus alleen deuren en ramen in beeld brengen als dit strikt nodig is en geen voorbijgangers vastleggen. Deze willen onbespied blijven en de exploitanten zijn ook niet de bewaker van de openbare weg.

Op grond van welke bevoegdheid wordt geopereerd?

Het gaat bij het gebruik van camera's voor toezicht en beveiliging om het verwerken van persoonsgegevens. Dit kan gebeuren door overheden en bedrijven. Voor de gemeente en andere overheden geldt hierbij als norm dat de verwerking noodzakelijk is voor de goede vervulling van de publiekrechtelijke taak; bij de politie is dit de politietaak. Aan alle elementen hiervan moet worden voldaan. Allereerst dient de noodzaak voldoende te worden onderbouwd. In Leeuwarden kwam de gemeenteraad tot een andere conclusie dan in Groningen. In Den Haag was met name de selectieve inzet een aandachtspunt.

Een gemeente zal het zorgdragen voor toezicht in de publieke ruimten doorgaans terecht tot haar publiekrechtelijke taak rekenen. Dit geldt ook voor de politie. Anders komt dit te liggen bij particuliere ondernemingen die het toezicht op de openbare ruimten – mede – tot hun taak rekenen. Voor hen geldt de norm dat zij persoonsgegevens, dus ook videobeelden, mogen verwerken voor hun gerechtvaardigd belang, tenzij de belangen of de fundamentele rechten prevaleren van degene die in beeld wordt gebracht. De bewaking van de voordeur van een bedrijf, zelfs van een bordeel, kan zo'n gerechtvaardigd belang zijn. Maar het opnemen van de passanten is slechts aanvaardbaar als dit hiermee onvermijdelijk samenvalt.

Tegen verdergaande registratie zullen zich al snel de belangen, waaronder het recht op privacybescherming, van deze passanten verzetten. Er is hierbij sprake

van een glijdende schaal. Bij bedrijventerreinen omsluit de beveiliging bijna altijd ook de bewaking van de openbare weg. De inbreuk op belangen en rechten van bezoekers speelt hier minder een rol dan in de 'warmere buurten'. Dus is het gerechtvaardigd belang van de ondernemers op dit terrein al veel sterker om het toezicht op de openbare weg 'mee te nemen'.

Maar dit betekent niet dat de overheid daarmee haar bevoegdheid kwijtraakt. Het gerechtvaardigd particulier belang en de uitoefening van de publiekrechtelijke taak gaan in deze situaties gelijk op. In het algemeen geldt dat een grens tussen het publieke en private domein niet altijd scherp valt te trekken. In de kern behoudt dit onderscheid evenwel zijn waarde. Ook de politiek spreekt bij herhaling uit dat voor particuliere ondernemers in beginsel geen taak ligt in het door beveiligingsorganisaties laten bewaken van openbare ruimten.

Welk doel wordt nagestreefd?

Het vastleggen van het doel of de doelen van de inzet van videocamera-systemen is essentieel voor het onderbouwen van de noodzaak ervan en voor het normeren van het – verdergaand – gebruik ervan. Voor dit laatste vormt het doel waarvoor de beelden zijn verzameld het toetsingskader. Welk doel gesteld kan worden wordt bepaald door de bevoegdheid om opnamen te maken. Is dit vanuit een publiekrechtelijke taak van de gemeente voor het integraal veiligheidsbeleid? Is het een ondernemersbelang? Of is sprake van uitoefening van de politietaak?

Het doel waarvoor de beelden worden vastgelegd is ook bepalend voor de vraag welk verdergaande gebruik van de beelden mag worden gemaakt. Verdergaand gebruik is toegestaan als het verenigbaar met het doel of de doelen waarvoor de beelden werden verzameld. In de gemeente Groningen is ervoor gekozen om de registratie van videobeelden te baseren op de Wet politieregisters. Dit maakt het mogelijk dat de videobeelden worden aangewend voor het brede takenpakket van de politie:

1. In het kader van de uitvoering van artikel 2 van de Politiewet 1993 heeft het register tot doel de informatievoorziening binnen het korps mogelijk te maken voor zover het betreft het met behulp van camera's uitoefenen van toezicht op het bij besluit van de Gemeenteraad Groningen vastgesteld gebied van de gemeente Groningen:
   a. ter voorkoming van misdrijven;
   b. ter voorkoming van verstoringen van de openbare orde;
   c. het in voorkomende gevallen bereiken van een efficiënte hulpverlening door hulpverleningsdiensten:
   d. het bij het constateren van strafbare feiten het identificeren en het opsporen van de dader(s);
   e. het beschikbaar stellen van deze gegevens aan het Openbaar Ministerie voor zover het dient ter bewijsvoering.
2. Het register heeft ten doel de gegevens te gebruiken ten behoeve van interne bedrijfsstatistiek, interne bedrijfsvoering en interne ontwikkeling van beleid met betrekking tot de uitvoering van de politietaak.

Met de brede taakstelling van de politie is deze ruime doelomschrijving in overeenstemming. Maar in waarborgen is voorzien. Het gebruik van de informatie die de politie in het kader van dit toezicht verzamelt, blijft in beginsel binnen de eigen organisatie. De Wet politieregisters kent een zogenaamd gesloten verstrekkingenregime. Uitwisseling met buitenstaanders is doorgaans alleen maar mogelijk als dit noodzakelijk is voor de uitoefening van de politietaak. Deze beperking geldt dus voor de uitwisseling van beelden met

bijvoorbeeld winkeliers of horecaondernemers om een toegangsverbod te realiseren.

Andere oplossingen zijn goed denkbaar. Zo heeft de gemeente Ede het cameratoezicht in het kader van integraal veiligheidsbeleid als taak van het college van B&W aangemerkt en hiermee de registratie onder de verantwoordelijkheid van dit college gebracht. Op deze wijze geeft zij invulling aan haar publiekrechtelijke taakuitoefening. De gemeente Amsterdam heeft voor een gemengd stelsel gekozen. Het toezicht in – kort gezegd – de binnenstad wordt exclusief onder de politietaak gebracht. In de overige stadsdelen oefent de gemeente op grond van haar publiekrechtelijke taakuitoefening toezicht uit.

In de toekomst zal de vraag vaker gaan spelen naar de mogelijkheden van samenwerking van politie en plaatselijke overheden bij het effectueren van veiligheidsbeleid, onder meer bij toezicht door videocamera's. Nu is het vaak nog beperkt tot bedrijventerreinen, maar de kwestie speelt steeds meer ook bij uitgaans- en winkelcentra Rode draad hierbij dient te zijn dat ieder zijn verantwoordelijkheid behoudt en binnen het kader daarvan aan de samenwerking gestalte geeft. De speelruimte voor samenwerking in een convenant of arrangement wordt dan ook bepaald door de bevoegdheid hiertoe van de deelnemende partijen. De overheid of de politie kunnen hieraan deelnemen vanuit hun publiekrechtelijke taakuitoefening. Deze kan parallel lopen aan gerechtvaardigde belangen van bedrijven. Als dat is vastgesteld dan kan een convenant of een arrangement een goede gelegenheid zijn om de samenwerking bij de uitoefening van het toezicht vorm te geven.

Wie voert de regie?

Uit de bevoegdheid voor het door videobeelden verzamelen van persoonsgegevens volgt wie verantwoordelijk is voor de uitvoering. De vraag naar de regie wordt in juridische termen bepaald door wie de houder van de registratie van het beeldmateriaal, of – onder nieuwe Wet bescherming persoonsgegevens – wie de 'verantwoordelijke' is. Bij een gemeente kan dit de burgemeester zijn vanuit zijn verantwoordelijkheid voor de openbare orde dan wel het gemeentebestuur in bredere zin. Als het beeldmateriaal in een politieregister wordt opgeslagen dan volgt uit de Wet politieregisters dat de korpsbeheerder – de burgemeester van de hoofdplaats uit de regio – dat is. In alle gevallen gaat het om de autoriteit die zeggenschap heeft over het systeem van camerabewaking.

Dit betekent niet dat de uitvoering van het toezicht ook door de verantwoordelijke organisaties zelf dient te geschieden. Uitbesteding van het bekijken van de beelden aan bijvoorbeeld een meldkamer van een particuliere beveiligingsorganisatie is mogelijk. Juist in situaties waarin sprake is van parallelle bevoegdheden van de overheid en bedrijven kan dit een oplossing zijn. Denk hierbij aan het toezicht op bedrijventerreinen. De verantwoordelijkheid van de overheid voor het toezicht in het publieke domein moet in zo'n samenwerkingsverband wel duidelijk tot uitdrukking komen.

Bij uitbesteding van de uitvoering van directe toezicht moeten ook waarborgen worden ingebouwd dat de verantwoordelijke voor het toezicht de zeggenschap houdt over het gebruik van de videobeelden die in het kader van zijn bevoegdheid worden verzameld. Registratie in één meldkamer mag niet leiden tot ongeoorloofd uitwisseling van beeldmateriaal. Dit risico ligt natuurlijk op de loer. Hierover dienen dan ook heldere afspraken te worden gemaakt en vastgelegd.

Is er samenhang met andere maatregelen?

Een goede taakvervulling kenmerkt zich doordat cameratoezicht niet een geïsoleerde maatregel is, maar deel uitmaakt van een breder pakket van maatregelen dat gericht is op het houden van toezicht. Met het installeren van camera's alleen vergroot de overheid de veiligheid op straat nog niet en dat is meestal de voornaamste reden om camera's te installeren. Het vastleggen van videobeelden in het kader van een lokaal veiligheidsbeleid is doorgaans alleen maar effectief als dit gekoppeld is aan het inzetten van mensen. Meer 'blauw op straat' zoals in de gemeente Groningen is gerealiseerd, is dan ook meestal een noodzakelijke voorwaarde. Als zich incidenten voordoen dan verwacht de burger immers dat er wordt opgetreden.

Meestal vergen camera dus extra personeel op straat en in de meldkamer. Ook in andere opzicht kosten camera's – extra – geld. In Groningen werd niet alleen het aantal surveillerende agenten tijdens uitgaansavonden drastisch verhoogd maar ook het niveau van de straatverlichting. Ook leveren camera's extra werk op. Er worden meer incidenten geregistreerd en de burger mag dan ook een reactie van de overheid hierop verwachten.

Wordt het bekend gemaakt?

Een belangrijk element van de bescherming van persoonsgegevens is dat de burger weet wat er met zijn persoonsgegevens gebeurt. Hierin is in de privacywetgeving voorzien door het opnemen van de verplichting voor degene die met persoonsgegevens omgaat om de betrokkene hierover te informeren. In overeenstemming hiermee is de (uitbreiding van de) strafbaarstelling van het heimelijk observeren van het publiek. In de praktijk wordt dit gerealiseerd door het plaatsen van waarschuwingsborden, waarvan ook nog een preventief effect kan uitgaan. De Registratiekamer verwelkomt deze uitbreiding.

Van even groot belang is echter dat de beslissing tot het invoeren van cameratoezicht wordt genomen na een publiek debat hierover te hebben gevoerd. Cameratoezicht met name in stadscentra leent zich hiervoor uitstekend zoals is in diverse gemeenten is gebleken. Zowel in Groningen als in Leeuwarden is de beslissing om al dan niet camera's te plaatsen genomen na uitvoerige discussie in en buiten de gemeenteraad. Ook de individuele burger van wie opname zijn gemaakt, heeft overigens recht op informatie hierover. De uitoefening van het in de privacywetgeving verankerde inzagerecht geldt ook voor video-opnamen.

Een laatste element van bekendmaking betreft de aanmelding van de verwerking van videobeelden bij het – toekomstige – College bescherming persoonsgegevens. De bedoeling hiervan is dat voor iedere geïnteresseerde burger kan worden nagegaan op welke wijze door welke instantie en voor welk doel persoonsgegevens worden verzameld. Deze transparantie stelt hem ook in staat zijn privacyrechten, met name het kunnen kennisnemen van het over hem verzamelde materiaal en het eventueel verzoeken om verwijdering hiervan, uit te oefenen.

Wordt maat gehouden?

Als het gaat om inbreuken op de privacy van burgers dan zijn deze alleen maar gerechtvaardigd als deze voldoen aan de beginselen van proportionaliteit en subsidiariteit: met andere woorden onderzoek de noodzaak van de inbreuk en lever maatwerk. Deze principes liggen ook ten grondslag aan de wetgeving ter bescherming van persoonsgegevens.

Deze vragen speelden ook al in de fase waarin over de aanleg van een camerasysteem moet worden beslist. Maar als eenmaal deze beslissing is genomen dan komt het erg aan op de selectieve inzet van cameraobservatie. Dit is overigens niet alleen aan kwestie van privacybescherming, maar raakt ook de beheersing van de kosten van materieel en de inzet van personeel.

Naar tijd, plaats en aantal dienen camera's selectief te worden ingezet. Ook de reikwijdte en de mate van detaillering (inzoommogelijkheid) dienen te worden bepaald. Het doel is hierbij alles bepalend. Soms zal 24-uurscontrole noodzakelijk zijn, maar dit geldt niet in uitgaanscentra en evenmin in voetbalstadions. Voor verkeerstoezicht zal met globale beelden kunnen worden volstaan, tenzij het bekeuren op kenteken ook een doel van het cameratoezicht is. Ook de noodzaak van direct meekijken moet worden onderbouwd. Maar het niet-meekijken om kostenaspecten kan cameraobservatie ineffectief maken. Hiermee kan de rechtvaardiging van het gebruik in gevaar komen.

Niet vergeten mag worden om regelmatig de wijze van toezicht te evalueren en zonodig bij te stellen. Proportionaliteit en subsidiariteit worden ook bepaald door de inbedding van cameratoezicht in een samenstel van maatregelen. Maatvoering geldt ook bij de bewaartermijn. Het uitgangspunt van de Registratiekamer in haar rapport In beeld gebracht is een termijn van 24 uur. Indien cameratoezicht wordt gebruikt om toezicht te houden en voor beveiliging zorg te dragen in een bepaalde ruimte en in een bepaalde periode geen incidenten hebben plaatsgevonden, is er doorgaans geen reden om de gemaakte opnamen langer te bewaren. Deze zullen dan ook uit de registratie verwijderd en vernietigd moeten worden. De noodzaak van een langere bewaartermijn moet worden onderbouwd. Het kan zijn dat de constatering van incidenten niet altijd direct kan plaatsvinden. Alleen dan zal een langere termijn voor het bewaren van de opgenomen beelden gerechtvaardigd zijn.

Bestuurlijke kwesties

Er is geen weg terug, zo is de praktijk. Indien eenmaal door de verantwoordelijke autoriteiten is besloten tot het invoeren van camera's zal eerder de roep om meer dan om minder camera's klinken. In dat opzicht is van een verslaving al snel sprake. Des te groter is het belang dat over de normatieve vragen goed is nagedacht.

De camerasystemen worden ook steeds intelligenter. Detectiesystemen richten zich op het – tijdig – signaleren van risicogedrag. Datamining van videobeelden en koppeling met bestaande registraties maakt het mogelijk snel en trefzeker personen op te sporen.

Terug kan niet maar vooruit wel. En dat wil zeggen dat ook onder ogen moet worden gezien dat zich intelligentere toepassingen zullen aandienen. Vroeg of laat zullen de autoriteiten ook deze een plaats moeten geven. Enkele voorbeelden betreffen de koppeling van registraties, de detectie van verdacht gedrag en de samenvoeging van meldkamers.

Koppeling van videocamerasystemen met andere registraties, zoals het kenteken- of het opsporingsregister, zal tot een aanscherping van het toezicht leiden. De inzet van camera's zal geleidelijk aan verschuiven van preventieve naar meer repressieve functies. Bij de besluitvorming over de inzet van dergelijke systemen dient dit aspect uitdrukkelijk te worden betrokken. De acceptatie door de burger van dergelijke systemen kan nadelig worden beïnvloed door een te sterke oriëntatie op deze repressieve functies.

Intelligente toepassingen van camerasystemen presenteren slechts die informatie die relevant is voor het doel van de registratie. Er is steeds meer behoefte aan het vroegtijdig herkennen van verdachte situaties. Technisch wordt het mogelijk dergelijke gedraging te definiëren en alleen de beelden die daarop betrekking hebben, aan de met het cameratoezicht belaste waarnemers te presenteren. Het debat zal zich dan concentreren op de vraag wat ongewenst gedrag is. De doelstelling die aan het inrichten van het cameratoezicht ten grondslag lagen, zal dan bepalend zijn voor de wijze van inzet van dergelijke detectiesystemen. Gericht gebruik van videobeelden maakt onmiskenbaar een grotere inbreuk op de privacy van enkelen, maar heeft als voordeel dat het registeren van 'niet-verdachte' personen overbodig wordt.

Een andere toepassingsvorm die voor de privacybescherming maar ook voor de bestuurlijke controle van belang is, is de inrichting van meldkamers. Het handhaven van de regie zal meer onder druk komen te staan maarmate de registratie op grotere schaal plaatsvindt.

Over kijkhuizen en kijkdozen

Cameraobservatie is in onze maatschappij niet meer weg te denken. De voordelen hiervan zijn nu nog overheersend. Het effect van cameratoezicht wordt versterkt door de inrichting van centrale meldkamers. Hierin worden bijvoorbeeld alle beelden van de NS-stations bekeken. Maar de opkomst van intelligentere systemen en de groeiende tendens tot het centraliseren van het toezicht zijn ontwikkelingen die de voordelen in nadelen voor de burger kunnen doen omslaan. Zeker als de belangstelling van de politie groeit om van al deze systemen gebruik te maken.

Cameraobservatie in de openbare ruimten wordt met name gerechtvaardigd vanwege de bijdrage aan de gevoelens van veiligheid van de burger. Wanneer deze observatie gaat verworden tot een veelomvattend volgsysteem van dezelfde burger kan deze de hiermee gepaard gaande inbreuk op zijn privacy wel eens als een bedreiging van zijn veiligheid beschouwen. Dit geldt des te sterker naarmate de mogelijkheden toenemen om ongewenst gedrag trefzeker te ontdekken.

Er wordt al gesproken over KIJKHUIZEN. Zo'n term roept negatievere associaties op dan de klassieke meldkamer, maar geeft ook meteen het verschil hiermee treffend weer. De wereld wordt dan tot een KIJKDOOS, waarin de burgers niet langer gezien maar wel bekeken worden.

thema

Veranderingen in de gezondheidszorg

Op het terrein van de gezondheidszorg zijn veranderingen gaande die vergaande gevolgen kunnen hebben voor de wijze waarop die zorg in de nabije toekomst wordt verleend, bestuurd en gefinancierd. Het streven staat hierbij voorop om te komen tot betere kwaliteit, grotere toegankelijkheid, meer efficiency en duurzame financiering, voor iedereen die zorg behoeft. Schaalvergroting en marktwerking staan hierbij hoog in het vaandel. Een belangrijke rol in dat verband speelt de inzet van informatie- en communicatietechnologie (ICT) om het toenemende gegevensverkeer binnen de sector in goede banen te leiden. Helaas wordt daarbij echter te weinig nagedacht over de bescherming van persoonsgegevens en het medisch beroepsgeheim. De randvoorwaarden die de wetgeving op dit gebied stelt, worden in elk geval door diverse partijen in de zorg stelselmatig te licht opgevat. Andere belangrijke uitgangspunten van de gezondheidszorg kunnen daardoor in de verdrukking komen.

Informatie in de zorg

De zorgvuldige omgang met vertrouwelijke gegevens van patiënten is altijd een belangrijk aandachtspunt geweest in de gezondheidszorg. Het medisch beroepsgeheim staat daarbij centraal. Dit berust op het uitgangspunt dat iedereen zich om hulp of advies tot een arts of een andere hulpverlener moet kunnen wenden zonder de vrees dat informatie die hij of zij in dat kader aan de betrokken hulpverlener toevertrouwt, bij een ander bekend wordt. Duidelijkheid over de reikwijdte en de consequenties van het beroepsgeheim is in het belang van iedere patiënt en van de samenleving als geheel. Zorg voor de patiënt en zorg voor de informatie over de patiënt zijn in de gezondheidszorg nu eenmaal nauw verweven.

Hoewel de zorg voor de gezondheid nog steeds voorop staat, kan de gezondheidszorg steeds meer worden beschreven als een 'informatieverwerkend proces'. Daarbij wordt informatie over patiënten verzameld, vastgelegd, toegankelijk gemaakt en uitgewisseld, en wordt ook voortdurend nieuwe informatie over patiënten gegenereerd en in de verwerkingen betrokken. Dit geldt voor het 'primaire proces' – het leveren van zorg – maar het geldt ook en in sterkere mate voor de samenhangende processen van beheer, financiering, medisch-wetenschappelijk onderzoek en ontwikkeling van beleid. Vanaf het moment dat een patiënt zich wendt tot een huisarts of medisch specialist, is er sprake van een constante stroom van gegevens, die maar ten dele verband houdt met het primaire proces. Elektronische dossiervorming vindt intussen op grote schaal plaats. Niet alleen bij huisartsen en apotheken, maar bijvoorbeeld ook in de geestelijke gezondheidszorg.

In september 2000 hebben koepels van patiënten, zorgaanbieders, zorgverleners, zorgverzekeraars en de ministeries van Economische Zaken en Volksgezondheid, Welzijn en Sport (VWS) de Intentieverklaring van het ICT Platform in de Zorg (IPZorg) ondertekend. In november 2000 verscheen de *Beleidsbrief en Actieplan ICT in de Zorg* van de minister van VWS. Uit beide documenten blijkt dat de betrokken partijen een hoge ambitie hebben bij de toepassing van ICT in de gezondheidszorg en dat privacybescherming en beveiliging volgens alle partijen zeer zwaar dienen te wegen.

De minister van VWS wil dat de Registratiekamer bij het ontwikkelen van alle voornemens betrokken wordt. Hoewel dit uitgangspunt aanspreekt, laat dit de eigen verantwoordelijkheid van de betrokken partijen onverlet. Zij dienen elk voor zich zorg te dragen voor een adequate bescherming van de persoonsgegevens in de zorg.

Naast ambities voor ICT in de zorg leiden toenemende marktwerking en schaalvergroting in de gezondheidszorg tot een toename van het gegevensverkeer. De verantwoordelijkheden voor de gegevensverwerkingen zijn daardoor aan het verschuiven. De tendens om, naast een toenemend gebruik van ICT, steeds meer over te laten aan de (verzekerings)markt leidt in dit verband tot steeds meer problemen.

In dit hoofdstuk wordt de betrokkenheid van de Registratiekamer bij de hiervoor genoemde ontwikkelingen uiteengezet aan de hand van vier onderwerpen:
- voornemens omtrent ICT in de zorg;
- indicatiestelling AWBZ;
- wachtlijstregistraties en zorgtoewijzing;
- de positie van zorgverzekeraars.

Het hoofdstuk wordt afgesloten met een korte vooruitblik op de besluitvorming over het SER-advies dat in december 2000 is uitgebracht over de voorgenomen stelselherziening in de gezondheidszorg. Bij deze stelselherziening zal rekening dienen te worden gehouden met de wetgeving ter bescherming van persoonsgegevens en het medisch beroepsgeheim.

ICT in de zorg

In 2000 hebben diverse partijen in de gezondheidszorg onderzoek gedaan naar de randvoorwaarden voor ICT in de zorg, zoals een doeltreffende identificatie van patiënten en zorgverleners, een autorisatiestructuur voor de toegang tot vastgelegde gegevens en de opbouw van een virtueel elektronisch patiëntendossier (EPD). Gestreefd wordt naar een EPD waarmee, ongeacht tijdstip en locatie en onder strikte regels van autorisatie en bescherming van de privacy, toegang kan worden verkregen tot de relevante medische gegevens van patiënten. De Registratiekamer volgt deze ontwikkeling van nabij. Ter illustratie van haar betrokkenheid volgen vier voorbeelden.

Juridisch laboratorium

Het eerste voorbeeld is de deelname van de Registratiekamer aan het Juridisch Laboratorium van het programma *ICT in de Zorg* van ZorgOnderzoek Nederland (ZON). In dat verband heeft zij onder andere notities ingebracht over patiënten- en zorgverlenersidentificatie en de problematiek van verwijsindexen. Bij patiënten- en zorgverlenersidentificatie gaat het met name om persoonsnummers en gebruik van biometrie (een verzameling technieken gebaseerd op het meten van lichaamskenmerken die uniek zijn voor de drager ervan). Uit deze notitie blijkt onder andere dat naarmate het bereik van het patiëntenidentificatienummer groter is, het risico toeneemt dat de beginselen ter bescherming van persoonsgegevens geschonden worden.

Uit de notitie over verwijsindexen blijkt onder andere dat men zich eerst dient af te vragen of het gebruik van de verwijsindex noodzakelijk is. Zo ja, dan dienen de mogelijke risico's die aan verwijsindexen kleven, zo veel mogelijk te worden beperkt. Daarbij geldt als basisregel dat steeds een verantwoordelijke voor de verwijsindex dient te worden aangewezen. Deze dient ervoor te zorgen dat de verwijsindex zo min mogelijk persoonsgegevens bevat. Ieder persoonsgegeven dient hierbij te voldoen aan de in de notitie uitgewerkte wet- en regelgeving.

Advies over Intentieverklaring

Het tweede voorbeeld is het advies dat de Registratiekamer desgevraagd heeft uitgebracht over de genoemde Intentieverklaring van IPZorg. In dat advies geeft zij aan de voorgestelde stapsgewijze aanpak – via pilots – op zichzelf positief te vinden. Bij de uitvoering van deze voornemens dienen volgens de Registratiekamer echter nog wel wat hobbels te worden genomen. In het bijzonder vroeg de Registratiekamer aandacht voor de invoering van het Zorg Identificatie Nummer (ZIN). Het gaat hier om een onomkeerbare versleuteling van het sofi-nummer. Een dergelijke aanpak leidt, mits goed beveiligd, tot een doelgebonden nummer voor de gezondheidszorg. Bij de uitwerking van dit voornemen heeft de Registratiekamer, naast beveiligingsvragen, ook vragen gesteld over de betrouwbaarheid van het ZIN, de bevoegdheid van de verantwoordelijke voor de uitgifte van ZIN om over het sofi-nummer te beschikken en tenslotte nog gewezen op de behoefte aan wetgeving.

Onder meer in reactie op dit advies van de Registratiekamer heeft de minister van VWS in haar *Beleidsbrief ICT in de Zorg* laten weten, dat de introductie van een ZIN zal leiden tot aanpassing van bestaande wet- en regelgeving. Tevens heeft zij IPZorg de opdracht gegeven een plan van aanpak uit te werken voor de invoering van het ZIN. Dit plan van aanpak dient een voorstel te bevatten voor zowel de uitgifte- en beheersorganisatie, als voor de invoering van het nieuwe ZIN in alle bestaande informatiesystemen.

Biometrische experimenten

Het derde voorbeeld is dat de Registratiekamer op enige afstand als onafhankelijk adviseur betrokken is geweest bij biometrische experimenten, zoals de Landelijke Centrale Middelen Registratie, het Nederlands Brandwonden Informatiesysteem en de Parkinsonpas van de verzekeraar Zorg en Zekerheid te Leiden.

Zorgpas-project

Het vierde voorbeeld betreft de activiteiten van de Stichting Zorgpasgroep. Deze partij is door de minister van VWS aangewezen om in de gebieden waar de zorgverleners met elkaar verbonden zijn, te werken aan een infrastructuur die de relevante gegevens over patiënten beschikbaar kan stellen. Gestreefd wordt naar een chipcard in combinatie met de elektronische snelweg. Het Zorgpas-project is een initiatief van verzekeraars, zorgaanbieders en patiënten- en consumentenorganisaties. De Registratiekamer is als onafhankelijke deskundige op enige afstand bij dit project betrokken.

Indicatiestelling AWBZ

Gemeenten hebben de verantwoordelijkheid gekregen om op grond van de Algemene wet bijzondere ziektekosten (AWBZ) een onafhankelijk indicatieorgaan in te stellen. Iedereen die zorg nodig heeft van een zorgverlenende instelling, moet daarvoor een aanvraag indienen bij een regionaal indicatieorgaan (RIO). Dit RIO neemt de aanvraag in behandeling en bepaalt de zorgbehoefte op basis van gedetailleerde informatie die de zorgvrager en zorgverleners verstrekken over stoornissen en beperkingen van de betrokkene. In 2000 (en de twee voorgaande jaren) zijn bij de Registratiekamer diverse klachten en vragen binnengekomen in het kader van de indicatiestelling. Bijvoorbeeld over het, zonder medeweten van betrokkene, verstrekken van gegevens over de zorgvrager door een thuiszorginstelling aan een RIO. Of over het door RIO's verstrekken van gegevens die voor een ander doel, zoals indicatiestelling op grond van de Wet voorziening gehandicapten (WVG), waren verkregen.

Mede gelet op de vragen en klachten over de bescherming van persoonsgegevens bij indicatiestelling heeft de Registratiekamer in augustus 2000 het rapport *Zorg voor gegevens bij indicatiestelling* uitgebracht. Op dit terrein worden evidente spanningen aangetroffen tussen reeds in gang gezette ontwikkelingen enerzijds en de wetgeving ter bescherming van persoonsgegevens anderzijds. Voorbeelden van deze spanningen zijn in de eerste plaats het feit dat de vele specifieke plaatselijke of regionale vormen van indicatiestelling zodanig onderling van elkaar verschillen, dat voor de zorgvrager het hele proces van zorgvraag tot verlening van zorg ondoorzichtig is. Dit geldt niet alleen voor de gegevensverwerking, maar ook voor de vele wetten en regelingen die daarbij van belang zijn. Deze problematiek raakt ook de bescherming van de privacy op het punt van omgaan met gegevens van zorgvragers. In de tweede plaats brengt de geïntegreerde indicatiestelling binnen één RIO spanningen met zich mee ten aanzien van het verenigbaar gebruik van de verzamelde gegevens. In de derde plaats bevindt de indicatiestelling zich in het begin van de zorgketen. Daardoor blijkt bij RIO's in de praktijk de neiging te bestaan om meer gegevens te verzamelen dan noodzakelijk is voor hun eigen specifieke taak. Er worden ook alvast gegevens verzameld voor het mogelijk daarop volgende proces.

Wachtlijstbeheer en zorgtoewijzing

De Registratiekamer kreeg een plan onder ogen voor zorgtoewijzing en wachtlijstbeheer in de AWBZ. Het ministerie van VWS, Zorgverzekeraars Nederland (ZN) en het College van Zorgverzekeringen (CvZ) willen dat in de AWBZ-sectoren van elke patiënt gegevens worden verzameld over indicatie, zorgtoewijzing, gerealiseerde zorg en niet gerealiseerde zorg. Het zorgkantoor (de dominante zorgverzekeraar in een regio) zou de registratie voor zijn rekening moeten nemen. Vervolgens wordt er gestreefd naar een landelijk uniform systeem in de AWBZ-sectoren, via zorgkantoren en onder verantwoordelijkheid van het CvZ. Bij dit plan worden persoonsgegevens over cliënten verstrekt aan zorgkantoren voor twee doelen van geheel verschillende aard: het op *individueel* niveau koppelen van zorgvraag en zorgaanbod en het op *algemeen* niveau genereren van beleidsinformatie over wachtlijsten en wachttijden. Dit zou moeten leiden tot een AWBZ-brede zorgregistratie. Ook op dit algemene niveau zou men gebruik willen maken van unieke identificatie van de zorgvrager.

De Registratiekamer heeft de minister en de staatssecretaris van VWS en ZN erop gewezen dat zij ernstige twijfels heeft of de gegevensverstrekkingen in verband met die maatregelen een rechtmatige grondslag hebben, zowel waar het gaat om zorgaanbieders als waar het gaat om RIO's, zorgkantoren, VWS en het CvZ. Met name heeft de Registratiekamer kritische kanttekeningen geplaatst bij de voorgenomen landelijke AWBZ-brede zorgregistratie, waarbij het streven zou zijn deze registratie te voorzien van gegevens die tot op individueel niveau identificeerbaar zijn.

Uit eerdere publicaties van de Registratiekamer, zoals het rapport *Verstrekking van de ontslagdiagnosecode* uit 1993, het rapport Managed care uit 1998, en uit de inleiding die de voorzitter van de Registratiekamer op 25 september 2000 heeft uitgesproken tijdens een lunchbijeenkomst bij Zorgverzekeraars Nederland te Zeist komt naar voren dat een wezenlijk onderscheid gemaakt moet worden tussen het verstrekken van gegevens over cliënten in de zorg op *algemeen* c.q. geaggregeerd niveau en op *individueel* niveau. In het laatste geval zijn zowel de algemene privacywetgeving als de specifieke regels uit het gezondheidsrecht over gegevensverstrekking van toepassing.

Positie van zorgverzekeraars

Zorgverzekeraars krijgen, als organisaties buiten de directe zorgverlening, een steeds grotere rol toebedeeld door de politiek. Naast de genoemde tendens om steeds meer gebruik te maken van ICT is de introductie van meer marktwerking een andere tendens in de gezondheidszorg. Deze tendens leidt waarschijnlijk tot minder en in elk geval andere regels voor de inrichting en werking van de gezondheidszorg. Het vraagt echter ook om heldere grenzen over de ruimte die partijen in de zorg via onderlinge afspraken kunnen invullen, én om scherp toezicht om die grenzen te bewaken en waar nodig te accentueren. De Registratiekamer heeft sterk de indruk dat gevoelige informatie over patiënten en zorgverleners nog wel eens te gemakkelijk doorstroomt naar zorgverzekeraars. In het overleg met zorgverzekeraars streeft zij naar een verduidelijking van de grenzen op dit gebied. Hierna volgen enkele punten van aandacht waar de Registratiekamer in relatie tot de zorgverzekeraars bij betrokken is geweest.

Zelfregulering

Het eerste voorbeeld is dat ZN – in overleg met de Registratiekamer – naast de Gedragscode bescherming persoonsgegevens van het Verbond van Verzekeraars, een addendum heeft ontwikkeld voor de zorgverzekering. Ook heeft de Registratiekamer ZN gestimuleerd tot het opstellen van een zogeheten ‘oerschema’, waarin de gegevensstromen van de zorgverzekering in kaart zijn gebracht. Het addendum en het ‘oer-schema’ zijn een goede aanzet van ZN, maar de grenzen aan de inrichting van het gegevensverkeer binnen de gezondheidszorg en een adequaat toezicht hierop, zal uiteindelijk de wetgever moeten trekken en vervolgens door VWS, in samenspraak met de betrokken partijen en toezichthouders, in de praktijk georganiseerd moeten worden. Tot dat moment zal het gegevensverkeer zich moeten houden aan de geldende randvoorwaarden. Er is in dat opzicht dan ook een duidelijke grens aan de zelfregulering of het stimuleren van ontwikkelingen van onderop.

De zorgverzekeraars bevinden zich nu steeds meer in een spagaat. Het beleid gaat ervan uit dat zij op basis van hun kennis over medische consumptie en beschikbare financiële middelen sturend optreden. Het wezenlijke onderscheid tussen individuele en geaggregeerde gegevens wordt daarbij veelal niet duidelijk gemaakt. Voor de individuele gegevens van patiënten gelden echter strakke randvoorwaarden die zowel de verkrijging als het gebruik van die gegevens door verzekeraars aan banden leggen. Het systematisch doordenken van deze situatie blijft helaas uit. De Registratiekamer is van oordeel dat ook op basis van het eerder bedoelde onderscheid en met inachtneming daarvan, aanvaardbare sturingsrelaties in de zorg kunnen worden ontwikkeld. Het laten voortduren van de bestaande dubbelzinnigheid in het beleid kan slechts ontsporingen in de hand werken.

Deregulering

Het tweede voorbeeld is dat zorgverzekeraars te kennen hebben gegeven graag het voortouw te willen nemen bij het betaalbaar en toegankelijk houden van de farmaceutische zorg in ons land. Volgens het Financieele Dagblad van 15 april 2000 heeft de minister van VWS een ‘medicijnplan’ ontwikkeld om de zorgverzekeraars de verantwoordelijkheid te geven over het medicijnendossier. De verzekeraars zouden in dat kader instrumenten in handen krijgen om een doelmatiger gebruik van geneesmiddelen te bevorderen. Zo zouden zij mogen meekijken over de schouders van voorschrijvende artsen en specialisten. Er wordt aan gedacht een elektronisch voorschrijfsysteem verplicht te stellen, waarbij artsen de indicatie moeten vermelden op het recept. Om dit alles

mogelijk te maken komt er volgens het medicijnplan een dereguleringstraject over een brede linie.

De Registratiekamer heeft, als adviseur van de regering, bij de minister van VWS al grote terughoudendheid bepleit bij het voorgestelde dereguleringstraject ter vergroting van de verantwoordelijkheid van de zorgverzekeraars, voor zover de persoonlijke levenssfeer van patiënten en cliënten daarmee in het gedrang komt. Een nieuw bestel op dit gebied zal ten minste aan de eerder bedoelde uitgangspunten van privacybescherming moeten voldoen.

Stelselherziening in de gezondheidszorg

De Sociaal-Economische Raad (SER) heeft in december 2000 een advies uitgebracht waarin hij zijn visie geeft op de toekomstige inrichting van het stelsel van ziektekostenverzekeringen en de organisatie van de gezondheidszorg. De minister van VWS wil het advies van de SER betrekken bij het ontwikkelen van een langetermijnvisie op het zorg- en verzekeringsstelsel. De SER doet in zijn breed gedragen advies voorstellen over de modernisering van de AWBZ, de invoering van een algemene verzekering voor curatieve zorg waarbij de positie van de zorgverzekeraars naar de zorgaanbieders wordt versterkt, en een geleidelijke en zorgvuldige overgang naar een model van vraagsturing en marktwerking. De SER is zich ervan bewust dat deze voorstellen nadere invulling en uitwerking behoeven, alvorens een toekomstbestendig stelsel voor zorg en zekerheid vorm kan krijgen.

Bij alle genoemde voorstellen speelt de bescherming van persoonsgegevens een belangrijke rol. Het is van belang dat men zich bij de nadere invulling en uitwerking van het SER-advies rekenschap geeft van de verschillende rollen van de zorgverzekeraar, de andere partijen in de gezondheidszorg en de grenzen die in de wetgeving ter bescherming van persoonsgegevens en het medisch beroepsgeheim zijn gesteld. Deze rollen luisteren nauw en hebben gevolgen voor de inrichting van processen. Verheldering van rollen en grenzen is nodig, omdat er anders ontsporingen zullen plaatsvinden. Een zorgvuldige regie en daarmee sporende inrichting van systemen zijn daarbij van groot belang. Het is de hoogste tijd voor VWS, de zorgverzekeraars en de andere betrokken partijen om over deze ontwikkelingen na te denken en helderheid te scheppen.

In dit verband is het van belang dat de betrokken partijen zich realiseren dat de regels van de privacywetgeving en het beroepsgeheim van dwingend recht zijn, zodat de partijen in de zorg niet de mogelijkheid hebben om daarvan af te wijken. Ook nadere wetgeving op dit gebied zal in overeenstemming moeten zijn met de Europese privacyrichtlijn.

thema

Privacy op internet

De ups en downs van de 'internet-economie' zijn het afgelopen jaar duidelijk zichtbaar geworden. Geruchtmakende affaires rond geslaagde en minder geslaagde introducties van internetbedrijven op de beurs hebben hun stempel gedrukt op het beeld dat het publiek heeft van de verhoudingen binnen deze nieuwe wereld. Minder zichtbaar, maar onmiskenbaar duidelijk zijn de privacyproblemen die aan het toenemend gebruik van internet verbonden zijn. Beide invalshoeken – economie en privacy – blijken nauw met elkaar samen te hangen.

De marktwaarde van internetbedrijven werd in de loop van het jaar vooral bepaald door het vermogen om klanten – liefst grote aantallen klanten – aan zich te binden en daarmee een relatie te onderhouden. In de consumentenmarkt gaat het daarbij onherroepelijk ook om de zeggenschap over en toegang tot klantengegevens. Onderzoek in Europa en de Verenigde Staten laat tegelijk steeds weer zien dat de groei van elektronische handel en dienstverlening afhankelijk is van het vertrouwen bij de consument dat zijn gegevens bij de elektronische aanbieders in goede handen zijn. Goed beschouwd zal het succes van de internet-economie dus mede bepaald worden door de mate waarin de sector dat vertrouwen weet te veroveren én te behouden. Kortom: er in slaagt de privacyproblematiek tot een aanvaardbare oplossing te brengen.

Toegang tot veilig verkeer

Internet is een wereldomspannende verzameling van onderling verbonden computers, die het mogelijk maakt om een gigantische hoeveelheid informatie op te slaan en beschikbaar te stellen aan een breed publiek en daarop allerlei diensten aan te bieden variërend van e-mail tot elektronisch bankieren en steeds meer andere vormen van 'e-commerce' of 'e-government'.

Een typisch kenmerk van de huidige technologie op dit gebied is dat elke stap op internet zijn sporen nalaat: of het nu gaat om het raadplegen van openbare informatie of het verzenden van vertrouwelijke post, met simpele middelen en enige kennis van zaken zijn de gangen van betrokkenen gemakkelijk te traceren. Daarbij komt dat de veelheid van beschikbare vormen van communicatie op internet de mogelijkheid biedt tot vrijwel onbeperkt één-op-één verkeer met klanten of andere relaties. Samen leidt dit tot een exponentiële toename van het verkeer van persoonsgegevens op én rondom internet. De veilige afwikkeling van dat verkeer, met voldoende aandacht voor de privacy én andere fundamentele waarden van onze samenleving, is geen geringe opgave.

De meeste personen – in welke hoedanigheid ook – zullen voor het verkrijgen van toegang tot internet gebruik maken van de diensten van een internetprovider, dan wel van de faciliteiten van een werkgever of een andere derde, die op zijn beurt weer gebruik maakt van een internetprovider. De internetproviders – die naast eenvoudige toegang, meestal ook andere diensten leveren op dit gebied – zijn daarom te beschouwen als de poortwachters van internet. Alle andere partijen zijn ook via hen op internet aangesloten en communiceren langs die weg zowel met elkaar als met hun klanten.

De Registratiekamer heeft er dan ook voor gekozen om haar eerste onderzoeken op dit terrein te richten op de internetproviders. Daarnaast heeft zij bijzondere aandacht besteed aan de controle door werkgevers op het e-mail- en internetgebruik van hun werknemers. Omdat internet en de privacyproblematiek daaromheen naar hun aard een internationaal karakter hebben, heeft zij deze internationale dimensie vanaf het begin sterk benadrukt

door een nauwe samenwerking na te streven met zusterorganisaties in andere landen.

Rol van internetproviders

Aanleiding om een onderzoek in te stellen naar de wijze waarop aanbieders van toegang tot internet persoonsgegevens verzamelen en verder gebruiken, vormde een reclamecampagne van XS4all waarin eind 1999 de aandacht werd gevestigd op 'privacy' als relevant criterium voor een keuze tussen internetserviceproviders (ISP's). De reclamecampagne bracht twee concurrenten tot het aanspannen van een kort geding waarin niet duidelijk werd in hoeverre de gegevens van consumenten door providers worden gebruikt voor marketing- en reclame doeleinden, al dan niet voor derden. Deze hele gang van zaken voerde de Consumentenbond ertoe ook van haar kant aan te dringen op het instellen van een onderzoek.

Eind december 1999 heeft de Registratiekamer het onderzoek gestart en een vragenlijst verzonden aan zestig ISP's, waaronder zowel betaalde als gratis providers. Aanvullend heeft de Registratiekamer fact-finding onderzoeken uitgevoerd bij een aantal aanbieders van internetdiensten. Ook in deze onderzoeken zijn zowel betaalde als gratis providers betrokken.

De problematiek rondom het gebruik van persoonsgegevens door ISP's ondervindt ook in andere Europese landen de nodige aandacht. Daarom heeft de Registratiekamer besloten om de fact-finding onderzoeken op dit gebied uit te voeren in samenwerking met andere Europese zusterorganisaties, in het bijzonder met de Spaanse Registratiekamer (Agencia de Protección de Datos). Beide instellingen hebben gezamenlijk een plan van aanpak opgesteld. Het gebruik van dezelfde checklists en vragenlijsten in beide landen maakte het mogelijk om de resultaten van de onderzoeken makkelijk te vergelijken. Er werd gekozen voor drie onderzoeken naar internetproviders met een vergelijkbare profiel in elk land. De uitkomsten van de onderzoeken in beide landen kwamen in het algemeen met elkaar overeen. Toch waren er ook belangrijke verschillen: zo bleek dat Spaanse providers beter informatie gaven aan hun klanten dan de onderzochte Nederlandse ISP's en dat ze – anders dan de Nederlandse providers – in alle gevallen over een 'privacy policy' beschikten. Ook vroegen de Spaanse providers steeds toestemming aan hun abonnees om gegevens te mogen verstrekken aan andere bedrijven of business partners. Dit was niet het geval bij de onderzochte Nederlandse providers.

In het eerste kwartaal van het jaar 2000 zijn de teruggezonden vragenlijsten geïnventariseerd. De bevindingen van de Registratiekamer zijn in eerste instantie gebaseerd op de antwoorden van de providers. Daarnaast is gebruik gemaakt van informatiemateriaal, zoals algemene voorwaarden, informatiefolders en privacy policies die de providers aan de Registratiekamer hebben gezonden. De bevindingen van de fact-finding onderzoeken bij ISP's zijn betrokken bij de evaluatie van het algemene beeld.

Uit het onderzoek komt naar voren dat veel onduidelijkheid bestaat over het vastleggen en het gebruik van persoonsgegevens door de providers en dat deze zich dikwijls niet bewust zijn van de regels ter bescherming van de persoonlijke levenssfeer van hun abonnees. Door de Registratiekamer zijn op dit punt geen belangrijke verschillen waargenomen tussen de gratis en de betaalde providers.

Het is voor de abonnee in het algemeen moeilijk inzicht te krijgen in de wijze

waarop de provider met zijn persoonsgegevens omgaat. Bij aanmelding van de klant worden vaak meer gegevens gevraagd dan nodig is voor het aanbieden van toegang tot internet. De klant wordt niet duidelijk gemaakt waarvoor deze gegevens worden gebruikt. De onduidelijkheid wordt in de hand gewerkt door het feit dat de providers verschillende rollen spelen – naast toegang tot internet, leveren zij ook andere diensten aan abonnees en aan derden – en dat zij uit hoofde daarvan de beschikking krijgen over verschillende soorten van gegevens.

De providers die gratis toegang bieden, hanteren het 'voor wat hoort wat principe': tegenover gratis toegang staat het gebruik van abonneegegevens voor marketingdoeleinden. Ook de andere providers exploiteren echter klantgegevens. Voor zover het hierbij gaat om informatie over het gebruik door de klant van internet, is deze aan stringente wettelijke beperkingen onderworpen die in veel gevallen niet in acht worden genomen. Ook schiet de voorlichting ernstig tekort over de rechten die een klant heeft. Voorbeelden hiervan zijn het recht op kennisneming van de informatie die over hem verzameld wordt en het recht op verzet tegen direct marketing met zijn persoonsgegevens. De meerderheid van de providers sluit hun aansprakelijkheid voor de beveiliging van de persoonsgegevens uit. Dit is in strijd met de privacywetgeving, die juist een dwingendrechtelijk karakter heeft.

De Registratiekamer heeft uit haar onderzoek de conclusie getrokken dat de bescherming van persoonsgegevens door ISP's in aanzienlijke mate tekortschiet. In het rapport Klant in het Web heeft zij spelregels geformuleerd voor een adequaat privacybeleid bij het verlenen van internettoegang. Deze spelregels gaan onder andere over de soort gegevens die een provider bij het bieden van toegang tot internet mag vastleggen, het gebruik dat hij hiervan mag maken en de informatie die hij aan de klant moet verstrekken. Van groot belang is dat de informatie over het gebruik van internet door de klant aan stringente beperkingen blijft onderworpen. De klant moet erop kunnen vertrouwen dat hij in beginsel vrijelijk over internet kan surfen.

In het laatste stadium van het onderzoek is iedere provider afzonderlijk op de hoogte gesteld van de bevindingen die op zijn bedrijf betrekking hadden. De Vereniging van Nederlandse Internetproviders (NLIP) heeft naar aanleiding van het rapport van de Registratiekamer privacy als speerpunt voor het jaar 2001 gekozen. De Registratiekamer zal de resultaten daarvan met belangstelling volgen en zal daarnaar in een later stadium een gericht vervolgonderzoek doen.

Controle van werknemers

Het gebruik van e-mail en internet heeft binnen organisaties een grote vlucht genomen. Naast de evidente voordelen voor werkgever en werknemer, zoals productiviteit, bereikbaarheid en snelheid, hebben ook de negatieve kanten van deze media zich gemanifesteerd. Werkgevers hebben er daarom behoefte aan om het voorheen vrijblijvende gebruik van e-mail en internet in goede banen te leiden. Daarvoor worden gedragscodes en gebruiksregels opgesteld, die ook door middel van controle worden gehandhaafd.

Elektronische controle van computergebruik roept evenwel vragen op met betrekking tot de bescherming van de persoonlijke levenssfeer van de werknemer. Een groot aantal werkgevers, ondernemingsraden en individuele werknemers hebben deze vragen in de loop van het jaar voorgelegd aan de Registratiekamer. Op grond daarvan is een studie verricht naar de controle op

e-mail- en internetgebruik op het werk. Dit heeft in december 2000 geresulteerd in het rapport *Goed werken in netwerken.* Hierin wordt gepleit voor een evenwichtige en nuchtere benadering van dit onderwerp.

Met voorbeelden en praktijkgevallen zijn in het rapport allereerst de feitelijke en juridische achtergronden geschetst. Daaruit vloeien vuistregels voort die de werkgever een handvat bieden om een behoorlijk en zorgvuldig beleid vast te stellen. Het spreekt voor zich dat deze regels ook hun nut zullen hebben voor ondernemingsraden en individuele werknemers als het gaat om de beoordeling van het werkgeversbeleid en de consequenties daarvan voor hun privacy.

Op de werkplek levert de werknemer een deel van zijn privacy in. De werkgever mag dan ook controle uitoefenen op het gebruik van e-mail en internet op de werkplek. De impact van dit soort controle kan echter groot zijn. Daarom is maatwerk, afgestemd op de werksituatie en tot stand gekomen in nauw overleg met de ondernemingsraad, geboden. Heldere regels moeten werkgever en werknemer het noodzakelijke houvast bieden.

De vuistregels laten zien dat controle van e-mail op zichzelf niet is verboden. De werkgever is bevoegd om zekere voorwaarden te stellen aan het gebruik van e-mail-faciliteiten of bepaalde soorten van gebruik te verbieden. De werkgever zal dan wel de doeleinden moeten bepalen waarvoor hij controle noodzakelijk acht. De maatregelen moeten in een redelijke verhouding staan tot de belangen van de werknemer. Via e-mail zal de werknemer immers niet alleen zakelijk communiceren, maar in sommige gevallen ook privé-zaken afhandelen. Voorts zal de werknemer de ruimte moeten worden gelaten om zijn werkzaamheden naar eigen inzicht te verrichten zonder dat zijn baas voortdurend over zijn schouder meekijkt. Continue controle op e-mail doet daaraan afbreuk, zeker als die controle op de inhoud van de e-mail is gericht. Op grond van deze belangenafweging moet de werkgever vervolgens het minst vergaande middel kiezen.

Internetgebruik leidt weer tot andere risico's voor de werkgever en de werknemer. Voor de werkgever kan het gaan om de beveiliging van het netwerk, het tegengaan van verboden gebruik of het beschermen van andere bedrijfsbelangen, zoals bedrijfsgeheimen of de goede naam van de organisatie. Deze risico's doen de behoefte aan controle ontstaan. Voor de werknemer staat vaak diens privacy door de controle onder druk. Maar ook de vrijheid van meningsuiting of de informatievrijheid kan in het geding zijn.

Evenals controle op e-mail is controle op het internetgebruik van werknemers toegestaan. Met name is de werkgever bevoegd om voorwaarden te stellen aan het gebruik of bepaalde soorten van gebruik te verbieden. Ook hier geldt echter dat de genomen maatregelen in een redelijke verhouding moeten staan tot de belangen van werknemers en dat gebruikte middelen niet een verdergaande inbreuk mogen maken op die belangen dan strikt noodzakelijk is.

De inhoud van het rapport heeft in januari 2001 zeer veel aandacht getrokken. Het leek soms wel of veel mensen zich voor het eerst rekenschap gaven van de ambivalentie van moderne informatietechnologie: de voordelen én de nadelen daarvan zitten doorgaans dicht bij elkaar en doen zich bij onberaden toepassing ook allebei voor. De invoelbaarheid van deze spanning op de werkvloer droeg kennelijk bij aan de zeggingskracht van het rapport.

Europese Internet Task Force

In 1999 heeft de Werkgroep van nationale toezichthouders als bedoeld in artikel 29 van de Europese privacyrichtlijn, een expertgroep in het leven geroepen die zich specifiek richt op de uitleg van de relevante Europese richtlijnen voor het internetgebruik. Deze groep, bekend als de Internet Task Force (ITF), werd gecreëerd om kennis en expertise op internationaal niveau bij elkaar te brengen en gezamenlijk beleid te ontwikkelen op een gebied waar de nationale grenzen geen rol spelen.

Zoals werd aangekondigd in het jaarverslag 1999 (blz. 53) voorzag het werkprogramma van de ITF voor het jaar 2000 in een analyse over de werking van de Europese richtlijnen met betrekking tot de bescherming van persoonsgegevens op de meest voorkomende handelingen op internet. Dit doel is bereikt door middel van een omvangrijk document *Privacy on the Internet, An integrated EU approach to on-line data protection* aangenomen door de artikel 29 Werkgroep op 21 november 2000.

De Registratiekamer heeft een centrale rol gespeeld in de totstandkoming van dit document. De toezichthoudende autoriteiten van België, Denemarken, Duitsland, Frankrijk en Spanje hebben ook belangrijke bijdragen geleverd. Het document is begin 2001 gepresenteerd tijdens een hoorzitting van het Europese Parlement.

Het eerste hoofdstuk van het rapport geeft een technische beschrijving waarin wordt uitgelegd hoe internet in elkaar zit. Ook wordt de rol van de belangrijkste actoren aangegeven en worden de meest voorkomende internetdiensten beschreven. Het tweede hoofdstuk behandelt de juridische aspecten van internet en met name de reikwijdte van de algemene privacyrichtlijn 95/46/EG en de privacy- en telecommunicatierichtlijn 97/66/EG. Het belang van de thans lopende herziening van de telecommunicatieregelgeving op Europees niveau wordt hier benadrukt. Een uitgangspunt hierbij is dat beide bestaande richtlijnen van toepassing zijn op internet.

De volgende hoofdstukken van het rapport geven uitleg over de technische en juridische aspecten van internetdiensten, zoals e-mail, surfen en zoeken, nieuwsgroepen en chatrooms, elektronische transacties en cybermarketing (in het bijzonder het gebruik van banners). Elk hoofdstuk beschrijft ook de specifieke technische maatregelen die genomen kunnen worden om de privacy van de gebruikers beter te beschermen ('Privacy-Enhancing Technologies'). Een uitgebreide beschrijving van deze maatregelen is vervat in een apart hoofdstuk van het rapport.

Het laatste hoofdstuk van het rapport schetst een beeld van de belangrijkste trends en risico's uit privacy-oogpunt, die gelden voor alle on-line diensten. Door het groeiende aantal diensten wordt internet steeds onoverzichtelijker voor de consument. Internetbedrijven proberen hun diensten aantrekkelijk te maken voor gebruikers door ze te personaliseren. Hiervoor hebben ze persoonsgegevens nodig. Anoniem zijn op internet wordt daarenboven steeds moeilijker. Nieuwe technologieën maken het traceren van internetgebruikers eenvoudig door gebruik van statische IP-adressen, moderne software pakketten ('ET software'), 'cookies' en dergelijke. Persoonsgegevens worden geconcentreerd bij een klein aantal internetspelers, die met behulp van data mining technieken de gegevens kunnen verwerken en aldus verborgen links en kenmerken van gebruikers kunnen ontdekken. De gebruikers zijn zich hiervan

in de regel niet bewust. Het bewaren van bepaalde persoonsgegevens (bijvoorbeeld berichten uit nieuwsgroepen) voor zeer lange perioden, brengt extra risico's met zich mee.

In de conclusies van het rapport worden vier beleidslijnen voorgesteld:
– Vergroting van de privacybewustheid van internetgebruikers.
– Gecoördineerde toepassing van adequate wettelijke regels.
– Gebruik van privacy-conforme en privacy beschermende technologieën.
– Ontwikkeling van betrouwbare systemen voor controle en feedback.

Privacy-bewustwording

Het is van vitaal belang dat internetgebruikers voldoende informatie krijgen om zelf goed geïnformeerde keuzes te kunnen maken voor hun on-line activiteiten. Transparantie is dus doorslaggevend op dit gebied. Een aantal actoren op internet kunnen hierin een rol spelen.

Alle verantwoordelijken die on-line persoonsgegevens verzamelen, moeten ervoor zorgen dat informatie gegeven wordt aan de gebruikers telkens als gegevens verzameld worden (conform artikel 10 van Richtlijn 95/46/EG). Naast het plaatsen van een informatieve 'privacy policy' op de betrokken websites is het van betekenis dat op het moment van gegevensverzameling op een simpele en toegankelijke manier informatie aan de gebruikers wordt gegeven. Dit kan bijvoorbeeld gebeuren door gebruik van een box prompt die op het scherm van de gebruiker verschijnt.

Bedrijven die on-line activiteiten ontplooien, moeten zich realiseren dat de naleving van de bestaande privacyregels niet alleen van belang is vanuit het juridisch perspectief, maar ook als marketinginstrument in de informatiemaatschappij. Goed privacybeleid kan het vertrouwen van de consument winnen. Hier geldt dus: *'e-commerce + e-privacy = e-confidence'*. Overheidsinstanties die on-line opereren, hebben een voorbeeldfunctie en moeten daarom adequate maatregelen nemen om de privacy van gebruikers te garanderen in hun eigen toepassingen (zoals e-government). Daarnaast spelen overheidsinstanties een belangrijke rol in het bewustwordingsproces van de burgers aangaande de bestaande risico's van het internetgebruik en de rechten en verplichtingen van internetgebruikers en dienstenaanbieders.

Consumentenverenigingen en koepelorganisaties kunnen naast het informeren van hun leden, het monitoren van de activiteiten van invloedrijke actoren in de sector, zoals internetproviders op zich nemen. Uiteindelijk moeten de internetgebruikers echter zelf bepalen of ze gebruik willen maken van de aangeboden internetdiensten en onder welke voorwaarden.

Wettelijk kader

Het internationale karakter van internet maakt een gecoördineerde toepassing van de Europese regels op dit gebied onontbeerlijk. De Werkgroep artikel 29 speelt hierin een belangrijke rol. In dit kader is de herziening van Richtlijn 97/66/EG betreffende privacy en telecommunicatie, die door de Europese Commissie in gang is gezet om de richtlijn op een aantal punten in het licht van de technologische ontwikkeling te verduidelijken, van grote betekenis. Marktpartijen kunnen een belangrijke bijdrage leveren aan de ontwikkeling van zelfregulering in de internet- en e-commerce-sector binnen de aldus uitgezette kaders.

Privacy-technologie

Zowel de technische configuratie van hardware- en softwarepakketten als de protocollen en technische standaards bepalen grotendeels hoe de internetcommunicatie plaatsvindt. Het is daarom cruciaal om rekening te houden met de privacyregels tijdens de ontwikkeling van nieuwe technische producten. In een maatschappij waar niet verwacht mag worden dat alle internetgebruikers voldoende technische kennis hebben om zelf de instellingen van hun computer of de configuratie van de gebruikte software of hardware aan te passen, moeten fabrikanten van zulke producten er voor zorgen dat de 'default' posities van hun producten het hoogst mogelijke niveau van privacybescherming bieden.

Technologieën moeten niet slechts gezien worden als een bedreiging voor de privacy van de gebruikers, maar ook als middelen die gebruikt kunnen worden om de uitoefening van de privacyrechten te versimpelen (bijv. on-line inzage) of om extra bescherming te bieden. Voorbeelden van zulke 'Privacy-Enhancing' technologieën zijn proxy servers, e-mail filters, cookie killers, en dergelijke. Deze technische middelen moeten beschikbaar zijn voor de gebruikers zonder onredelijke kosten. Zowel het bedrijfsleven als overheidsinstanties moeten investeren in de ontwikkeling, promotie en gebruik van zulke middelen.

Controle en feedback

Passende maatregelen moeten genomen worden om de naleving van bestaande regels en technische eisen te waarborgen. In eerste instantie hebben toezichthoudende autoriteiten als taak het monitoren van de activiteiten van de verschillende actoren op internet die on-line persoonsgegevens verzamelen en verwerken. Daarnaast zouden ook andere partijen door middel van zelf-monitoring en evaluatiesystemen een bijdrage kunnen leveren aan een beter niveau van bescherming. Systemen van certificering, zoals labels voor websites, zouden de gebruikers kunnen helpen te herkennen welke actoren adequate spelregels bieden.

Het rapport van de Internet Task Force moet gezien worden als een eerste stap op Europees niveau om de bewustwording van alle betrokken partijen te bevorderen. Het belangrijkste doel van het rapport was toegankelijke technische beschrijvingen en gedetailleerde uitleg over de toepassing van de Europese regels betreffende privacy voor specifieke internetdiensten te bieden. De discussies binnen de Internet Task Force en met de Europese Commissie, tijdens de voorbereiding van dit rapport, hebben ook positieve invloed gehad op de totstandkoming van het voorstel van de Commissie voor een aangepaste Europese richtlijn voor privacy en telecommunicatie.

De Registratiekamer zal zich in de komende tijd – zowel op nationaal als internationaal niveau – door het rapport van de Europese Internet Task Force laten inspireren.

Opsporing op internet

Aan het scheppen van een veilige omgeving op internet zitten nog andere aspecten. De snelle mogelijkheden tot communicatie via internet hebben ook geleid tot het ontstaan van nieuwe vormen van criminaliteit. Daarnaast maken ook personen met minder fraaie intenties gebruik van deze middelen om bestaande vormen van criminaliteit te ondersteunen of uit te breiden. Het is daarom begrijpelijk dat ook opsporingsinstanties en veiligheidsdiensten belangstelling hebben voor wat er op of rond internet gebeurt.

Een deel van de gedragingen waarnaar de belangstelling van deze diensten uitgaat, speelt zich af in het openbaar. Althans zichtbaar voor iedereen die de moeite neemt om kennis te nemen van wat op websites voorhanden is. De al dan niet systematische bewaking van deze websites kan worden beschouwd als een deel van de algemene taak waarvoor de betrokken diensten in het leven zijn geroepen. De populaire term 'elektronische snelwegen' mag echter niet doen vergeten dat een ander deel van de communicatie zich afspeelt langs wegen waarvoor andere uitgangspunten gelden, zoals vertrouwelijkheid en restrictief gebruik van gegevens over het afgewikkelde verkeer. Onderzoek op die terreinen vergt bijzondere bevoegdheden die met toereikende waarborgen dienen te zijn omkleed. De ratio daarvan is niet dat onderzoek naar ongewenst gedrag dient te worden bemoeilijkt, maar dat het vertrouwen van argeloze en onschuldige burgers dient te worden beschermd. Ook het vertrouwen van burgers in de veiligheid van elektronische dienstverlening is ermee gebaat dat zij niet het gevoel krijgen dat niet direct betrokkenen voortdurend kunnen meekijken. Dit doet zich voor als ten behoeve van de *eventuele* mogelijkheid van een gerechtvaardigd overheidsoptreden, voorzieningen in het leven worden geroepen die een permanente bewaking van vertrouwelijke communicatie tussen burgers of bedrijven mogelijk maken.

De Registratiekamer heeft in de loop van het afgelopen jaar enkele malen uiting gegeven aan bezorgdheid over de vraag of de noodzakelijke grenzen hier wel steeds voldoende scherp in het oog worden gehouden. Politie en justitie moeten kunnen optreden tegen het hacken van computers of het verspreiden van kinderporno op internet. Internationale samenwerking is daarbij onontbeerlijk. Het opsporen van dergelijke criminaliteit moet echter wel plaatsvinden binnen de grenzen van de rechtsstaat. Daartoe behoren ook de beginselen van proportionaliteit en subsidiariteit die in internationaal erkende grondrechten zijn vervat. Dat geldt evenzeer als het gaat om de opsporing van andere vormen van criminaliteit met behulp van gegevens die op of rond internet voorhanden zijn.

De Registratiekamer heeft er in een brief aan de vaste commissie voor Justitie uit de Tweede Kamer op aangedrongen, dat deze grenzen in acht worden genomen bij de voorbereiding in het kader van de Raad van Europa – met deelname van derde landen – van het Verdrag inzake Cybercrime. Voorkomen moet worden dat de samenwerking van de Nederlandse politie en justitie met instanties in het buitenland leidt tot het verruimen van bevoegdheden voor het onderscheppen van internetverkeer en daarmee tot het verlagen van het Nederlandse niveau van bescherming van grondrechten. Samenwerking met beheerders van private en publieke netwerken moet berusten op duidelijke wettelijke verplichtingen in plaats van op moeilijk controleerbare vrijwillige medewerking. Bestaande opsporingsbevoegdheden dienen niet zonder duidelijke noodzaak te worden uitgebreid. Verplichtingen tot het structureel en langdurig vastleggen van gegevens over alle internetverkeer gaan te ver en moeten daarom worden afgewezen.

De Europese conferentie van Data Protection Commissioners heeft in april 2000 in Stockholm duidelijk stelling genomen tegen voorstellen die ISP's zouden verplichten om stelselmatig verkeersgegevens te bewaren voor langere tijd dan nu is toegestaan, om opsporingsinstanties in staat te stellen daartoe zo nodig toegang te verkrijgen. De conferentie benadrukte in een verklaring dat een dergelijke verplichting een ontoelaatbare inbreuk zou vormen op artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Als de mogelijkheid zou worden geopend om

in concrete gevallen gegevens te bewaren, moet er in die gevallen sprake zijn van een duidelijke noodzaak daartoe, moet de bewaartermijn niet langer zijn dan noodzakelijk en moet er een heldere wettelijke grondslag voor bestaan.

Naar het oordeel van de Registratiekamer geldt hetzelfde indien in Europees verband – buiten het kader van de Raad van Europa – afspraken zouden worden gemaakt met een soortgelijke strekking. Zij blijft de internationale discussies op dit terrein dan ook nauwlettend volgen.

4sporen

Activiteiten van de Registratiekamer

Communicatie
Ontwikkeling van normen
Technologie
Handhaving

Communicatie

De taken van de Registratiekamer worden onderverdeeld in vier sporen, waarvan het eerste spoor gericht is op communicatie. Het publiek moet namelijk weten dat er privacywetgeving is en wat deze betekent. Door effectieve communicatie, waarin een site op internet centraal staat, wordt het belang van een zorgvuldig gebruik van persoonsgegevens voor steeds meer partijen duidelijk. Het publiek kan verder gebruik maken van de expertise die bij de medewerkers van de Registratiekamer aanwezig is. Om een snelle dienstverlening te garanderen is er een frontoffice opgericht. Daarnaast worden bijeenkomsten georganiseerd en verzorgen medewerkers lezingen en artikelen in vakbladen. Ook journalisten benaderen de Registratiekamer: ze zijn op zoek naar meer achtergrondinformatie of vragen naar een standpunt. Daarnaast wordt onderzoek gedaan naar nieuwe vraagstukken op het gebied van privacybescherming. De uitkomsten van zo'n onderzoek worden vaak in de serie 'Achtergrondstudies en verkenningen' gepubliceerd.

Internetsite

In 1999 heeft de Registratiekamer een eigen website op internet gelanceerd. In 2000 is de website niet alleen aangevuld met actuele informatie, maar ook met publicaties en uitspraken uit voorgaande jaren. Mede hierdoor is het aantal bezoekers van de internetsite gestaag gestegen: van minder dan 5.000 in januari tot ruim 10.000 in december.

Publicaties en uitspraken zijn met een zoekmachine eenvoudig te vinden. Daarnaast is het aantal veel voorkomende vragen op de internetsite uitgebreid. De huidige 84 vragen en antwoorden worden te zijner tijd aangepast aan de nieuwe privacywet, de Wet bescherming persoonsgegevens (WBP).

Het is mogelijk om voorlichtingsmateriaal te bestellen of gratis van internet af te halen. Hierdoor worden verschillende doelgroepen sneller en beter bediend. Om de website voor de bezoeker beter toegankelijk te maken, is het afgelopen jaar gestart met het ontwikkelen van een nieuwe website. Op de nieuwe site staan de werkterreinen van de Registratiekamer centraal.

Frontoffice

Burgers kunnen vragen en klachten voorleggen aan de Registratiekamer. Via het frontoffice worden deze op een klantvriendelijke manier beantwoord. Medewerkers van het frontoffice beantwoordden in het verslagjaar bijna 9000 telefonische vragen, 2000 meer dan een jaar eerder. Naast de telefonische vragen werden er zo'n 250 brieven en e-mailberichten beantwoord waarin vragen werden voorgelegd.

Er werden veel vragen gesteld over videocamerabewaking, internet en over de invoering van de WBP. De grootste stroom met vragen ging echter over het controleren van e-mail- en internetgebruik op de werkplek. Deze vragen werden niet alleen gesteld door leden van ondernemingsraden en systeembeheerders, maar ook door werkgevers. Van de veel voorkomende vragen worden door het frontoffice informatiebladen gemaakt, die op verzoek worden toegestuurd.

Naast de vragen om voorlichting kwamen er ook ongeveer 200 klachten en bemiddelingsverzoeken binnen. Veel burgers wilden weten welke persoonsgegevens een bedrijf over hen heeft geregistreerd en van wie ze de gegevens hebben gekregen. De klachten gingen voornamelijk over het onterecht verstrekken van persoonsgegevens door het ene bedrijf aan het andere bedrijf.

Backoffice

Het backoffice heeft afgelopen jaar veel tijd besteed aan het voorlichting geven over de Wet bescherming persoonsgegevens. Veel bedrijven wilden graag weten wat de consequenties zijn van de invoering van de nieuwe wet voor hun organisatie. Naast schriftelijke beantwoording van de vragen zijn er ook verschillende workshops bij instellingen gegeven.

Naar aanleiding van de vragen over het controleren van e-mail en internetgebruik op de werkplek is het rapport *Goed werken in netwerken* geschreven. In dit rapport worden richtlijnen gegeven voor het controleren van werknemers. Hierbij moet onder andere gedacht worden aan beperkte controle, instemming van de ondernemingsraad, bewaartermijnen en scheiding zakelijke mail en privé mail.

Veel burgers kwamen met de vraag waarom een mobiel telefoonabonnement wordt geweigerd. Voor veel mensen is het onduidelijk hoe hun krediet wordt bepaald. Om hierin duidelijkheid te scheppen naar de consument toe is het rapport *De gewaardeerde klant* uitgebracht. Hierin wordt tevens een handvat gegeven aan bedrijven om behoorlijk en zorgvuldig om te gaan met persoonsgegevens.

Lezingen en bijeenkomsten

Naast vragen van individuele burgers ontving de Registratiekamer verzoeken om gastcolleges, spreekbeurten of workshops te verzorgen voor groepen geïnteresseerden. Zo werden diverse brancheorganisaties, dienstverlenende instellingen en andere organisaties bezocht. Bijzonder nuttig en leerzaam was de aanwezigheid tijdens de Direct Marketingbeurs in Maastricht. Juist binnen de direct-marketingsector is het zorgvuldig omgaan met persoonsgegevens een kwaliteitsvoorwaarde. Er was grote belangstelling vanuit deze branche voor de informatie die op de stand werd verstrekt. Verder was de Registratiekamer aanwezig tijdens de Infosecuritybeurs in Utrecht en het Zorgcongres in Etten-Leur.

De Registratiekamer bezocht niet alleen bijeenkomsten, maar organiseerde deze ook zelf om overleg te voeren met belanghebbende partijen. In mei werd in samenwerking met het Openbaar Ministerie en de Taakorganisatie Vreemdelingenzorg een publiek debat over biometrie georganiseerd.

Auditaanpak

Het in 1999 gestarte samenwerkingsproject Auditaanpak werd succesvol afgerond. De intensieve samenwerking tussen marktpartijen (audit- en adviesorganisaties), koepelorganisaties van auditors en belanghebbenden (o.a. werknemers- en werkgeversorganisaties) en de Registratiekamer heeft geresulteerd in de volgende auditproducten: Quickscan, WBP Zelfevaluatie en Raamwerk Privacy Audit. Met behulp van deze producten zijn organisaties in staat om de kwaliteit van de maatregelen ter bescherming van persoonsgegevens zowel te analyseren als te optimaliseren. Als vervolg op het project Auditaanpak zijn betrokken partijen eind 2000 van start gegaan om de belangstelling voor een privacycertificaat te onderzoeken.

Artikelen

In het tijdschrift *Privacy & Informatie*, dat tweemaandelijks verschijnt, verzorgt de Registratiekamer sinds begin 1998 een katern waarin samenvattingen zijn opgenomen van de belangrijkste uitspraken en adviezen aan de regering. In het katern staat tevens een overzicht van recent verschenen publicaties. Het katern

is met name bedoeld voor beroepsmatig geïnteresseerden. Ook in het tijdschrift *Computerrecht* verschijnt tweemaandelijks een selectie van relevante samenvattingen.

Verder verzorgden leden en medewerkers van de Registratiekamer diverse artikelen in vakbladen en tijdschriften. In het tijdschrift *Privacy & Informatie* verscheen het artikel *(Op)sporen op internet: privacybescherming onder druk*. Over het opsporen van strafbare feiten op internet en de inbreuk die daarbij gemaakt wordt op de privacy van de gebruikers van internet. In het *Nederlands Juristenblad* verscheen onder meer een artikel over de wet bijzondere politieregisters. Hierin werden kanttekeningen geplaatst bij de nieuwe regelgeving voor de bijzondere politieregisters vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer. Een volledig overzicht van de gepubliceerde artikelen vindt u in bijlage 6.

Media

De mediavoorlichting diende als een belangrijk instrument om het brede publiek te informeren over de standpunten en activiteiten van de Registratiekamer. Gedurende het verslagjaar is de kamer ongeveer 500 keer benaderd door de schrijvende en audiovisuele pers. Tijdens de woordvoering wordt zo min mogelijk ingegaan op incidenten.

De Registratiekamer werkte in het verslagjaar mee aan verschillende televisie-uitzendingen. Vooral de uitzendingen over de hielprikjesdatabank, waar onder andere de NOS en de Wereldomroep aandacht aan schonken, deden veel stof opwaaien. Uit onderzoek bleek dat de databank geen persoonsregistratie in de zin van de Wet persoonsregistraties is. Desondanks heeft de Registratiekamer het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) aanbevelingen gedaan over het omgaan met persoonsgegevens. KRO-ontbijttelevisie heeft een aantal keren aandacht besteed aan de inbreuk op de privacy door het gebruik van bewakingscamera's waarbij een woordvoerder van de Registratiekamer werd geïnterviewd.

Publicaties in eigen beheer

Onderzoek van de Registratiekamer leidde tot een aantal publicaties die in eigen beheer werden uitgebracht. Zij doet dit onder andere om aandacht te vragen voor nieuwe ontwikkelingen waarbij de bescherming van persoonsgegevens in het geding is en om haar positie als gesprekspartner te verstevigen. Zo verscheen in juni 2000 het rapport *Klant in het Web*, over de privacywaarborgen voor internettoegang. In diezelfde maand verscheen eveneens het rapport *Politiegegevens beschermd*. In het rapport wordt een toelichting gegeven op het gesloten verstrekkingenregime van de Wet politieregisters.

In augustus 2000 verscheen de herdruk van het rapport *Privacy-Enhancing Technologies: the path to anonimity*. 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.

Het rapport *Herkomst van de klant* verscheen in oktober 2000. Dit rapport verkent het bestaande spanningsveld tussen het insluiten en uitsluiten van mensen op grond van ras of etniciteit bij de marketing van producten. Dit rapport en *De gewaardeerde klant* over kredietbeoordeling waarbij derden zijn

betrokken, zoals handelsinformatiebureaus, werden op de Direct Marketingbeurs gelanceerd.

De laatste jaren is in de financiële sector in toenemende mate sprake van verstrengeling van aanbieders, diensten en producten. Dit verschijnsel heeft evidente privacyaspecten en was daarom aanleiding om een fact finding onderzoek in te stellen naar de gegevensverwerking in financiële conglomeraten. De centrale vraag in dit onderzoek was hoe binnen deze conglomeraten feitelijk wordt omgegaan met persoonsgegevens en hoe de bescherming van de persoonlijke levenssfeer in de praktijk is vormgegeven. De resultaten van dit onderzoek zijn neergelegd in *Bankverzekeraars en privacy, gegevensverwerking in financiële conglomeraten.* Het onderzoek is in stuurgroepverband voorbereid met de andere betrokken toezichthouders. De Registratiekamer is zeer erkentelijk voor hun adviezen en steun.

Het rapport geeft een beeld van de huidige stand van zaken en ontwikkelingen, zoals die door de conglomeraten zijn geschetst. In het rapport worden hierbij kanttekeningen geplaatst in het licht van de bestaande privacywetgeving en de WBP, die in de loop van 2001 in werking zal treden. Waar beschermingsmaatregelen mogelijk aanscherping behoeven, worden in het rapport ook verbeterpunten zichtbaar.

Tot slot verscheen in december *Goed werken in netwerken, regels voor controle op e-mails en internetgebruik van werknemers.* In de publicatie wordt evenwicht gezocht tussen de belangen van de werkgever (controle) enerzijds en de belangen van de werknemer (zo min mogelijk inbreuk op zijn privacy) anderzijds. De Registratiekamer is niet tegen controle door de werkgever, maar wel tegen systematische controle. De werkgever moet niet constant over de schouder van zijn werknemer meekijken. Het evenwicht tussen de tegenstrijdige belangen van de werkgever en de werknemer wordt gevonden in maatwerk, dat afgestemd moet worden op de werksituatie en tot stand zijn gekomen in overleg met de ondernemingsraad. Heldere afspraken bieden zowel werkgever als werknemer houvast.

Een volledig overzicht van de door de Registratiekamer uitgebrachte publicaties vindt u in bijlagen 3 en 4.

Ontwikkeling van normen

De Registratiekamer draagt bij aan de ontwikkeling van nieuwe en de concretisering van bestaande normen. Deze normen werken het in de grondwet vastgelegde recht op eerbiediging van de persoonlijke levenssfeer uit, voor zover het de verwerking van persoonsgegevens betreft. Hieraan blijkt in de samenleving een groeiende behoefte te bestaan. Zowel de gaande als de komende wetgeving ter bescherming van persoonsgegevens bevat namelijk open en abstracte normen die in de praktijk geconcretiseerd dienen te worden. Dit geldt voor de Wet persoonsregistraties (WPR) maar ook voor de Wet bescherming persoonsgegevens (WBP), die in 2001 in werking treedt. Deze normen maken het mogelijk om telkenmale bij nieuwe ontwikkelingen aan de bescherming van persoonsgegevens specifieke invulling te geven.

Als toezichthouder op de WPR en verwante regelgeving rekent de Registratiekamer het bijdragen aan de ontwikkeling en concretisering van normen voor de omgang met persoonsgegevens tot haar belangrijkste taken. Zij doet dit op verschillende wijzen en bedient hierbij verschillende doelgroepen. Zij adviseert over wetsvoorstellen, heeft een rol in de ontwikkeling van privacygedragscodes, verkent de normen op specifieke deelterreinen en is beschikbaar voor burgers, bedrijven, organisaties en overheidsinstellingen die vragen of klachten hebben of verzoeken om bemiddeling in geschillen. In dit hoofdstuk wordt een overzicht gegeven van de belangrijkste activiteiten op deze terreinen, waarbij dit jaar vooral aandacht wordt besteed aan de adviezen over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. Het ligt voor de hand dat bij deze advisering doorgaans al vooruit is gelopen op het inwerking treden van de WBP.

Wetgevingsadviezen

Herinrichting van de sociale zekerheid

De overheid streeft naar meer maatwerk en efficiency in de uitvoering van de sociale zekerheid en is daarom bezig met de herinrichting van het stelsel van de sociale zekerheid. Na kritiek op de oorspronkelijke plannen zijn in het verslagjaar de herziene plannen van het kabinet voor de nieuwe uitvoeringsstructuur van de sociale zekerheid (Structuur Uitvoering Werk en Inkomen, SUWI II) voorgelegd aan de Registratiekamer. In tegenstelling tot de oorspronkelijke plannen wordt in SUWI II de uitvoering van de sociale verzekeringen geconcentreerd in het publiekrechtelijke domein. Deze concentratie betekent een verbeterde transparantie voor wat betreft het gegevensverkeer en minder overdrachtsmomenten. Dit komt de bescherming van persoonsgegevens ten goede.

Wel heeft de Registratiekamer in diverse adviezen aangedrongen op het formuleren van heldere bepalingen aangaande de informatie-uitwisseling. Het moet voor alle betrokken personen, instellingen en bedrijven duidelijk zijn welke informatie tussen welke actoren voor welke processen mag worden uitgewisseld. Het begrip “noodzakelijk voor de uitoefening van de taak” als grondslag voor omvangrijke informatieprocessen schiet tekort en confronteert de bij de uitvoering betrokkenen met onnodige vragen over de legitimatie van hun handelen. In de in behandeling zijnde wetsontwerpen is aan dit klemmende advies van de Registratiekamer nauwelijks uitvoering gegeven.

Reïntegratie

Bij de reïntegratie van uitkeringsgerechtigden wordt in SUWI II sterk de nadruk

gelegd op onderlinge samenwerking tussen de betrokken publieke en private partijen, zoals Arbo-diensten en reïntegratiebedrijven. De Registratiekamer vraagt aandacht voor de risico's die de gegevensstromen met zich meebrengen en de kwetsbare positie waarin de te reïntegreren betrokkene zich bevindt. Het gaat hier vaak om de verstrekking van gevoelige gegevens, zoals financiële gegevens, persoonlijke omstandigheden en de ziektegeschiedenis van de betrokkene. Voor de bij de reïntegratie betrokken instanties en bedrijven vormen deze gegevens het bedrijfskapitaal.

Voor de Registratiekamer is een reden tot zorg dat de informatie-uitwisseling tussen de verschillende instanties en bedrijven tot op heden niet duidelijk is geregeld. Er zijn geen heldere criteria over de vraag of, en zo ja in welke gevallen, gegevens kunnen of moeten worden uitgewisseld. De Registratiekamer dringt er daarom op aan de basisregels voor de gegevensuitwisseling bij reïntegratie vast te leggen bij wet in formele zin met een nadere uitwerking op het niveau van Algemene maatregel van bestuur. Dit systeem verdient de voorkeur boven een werkwijze die gebaseerd is op het vragen van toestemming aan de betrokkene. Gezien diens verplichting om gegevens af te staan en zijn afhankelijke positie komt de vrijwilligheid bij het geven van toestemming onder druk te staan. Bovendien komt regelgeving de transparantie van de gegevensuitwisseling ten goede.

Sofi-nummer

De Registratiekamer is voorstander van een terughoudend gebruik van het sofi-nummer. Dat wil zeggen dat het gebruik wordt beperkt tot het domein waarvoor het in het leven is geroepen: dat van de uitvoering van de sociale zekerheid en de belastingheffing. In dit domein past het voorstel van de minister van Sociale Zaken en Werkgelegenheid om het sofi-nummer te gebruiken bij het gegevensverkeer tussen de publieke opdrachtgevers enerzijds en de private reïntegratiebedrijven en Arbo-diensten anderzijds. Om een ongewenste uitwaaiering van het sofi-nummer naar andere domeinen te voorkomen, is een beperkende gebruiksbepaling noodzakelijk voor het gebruik van het sofi-nummer door de reïntegratiebedrijven, vooral waar het de uitbesteding van taken aan derden in het kader van de reïntegratieopdracht betreft.

Toezicht

Nu de publieke verzekeringen ingrijpend zijn veranderd worden de financiële hiaten die hierdoor ontstaan, zoals het 'WAO-gat' en het 'ANW-hiaat', in veel gevallen gedekt door aanvullende, private verzekeringen. Uitgewisselde gegevens zijn hierbij een mogelijke bron van inkomsten: zij kunnen voor deze en andere nieuwe doelen worden gebruikt. Dit verdergaande gebruik is in bepaalde gevallen niet uitgesloten. Ook hiervoor is echter een wettelijke grondslag onmisbaar. Uitgangspunt dient te zijn dat de gegevens slechts gebruikt worden voor het doel waarvoor ze verzameld waren: het uitvoeren van de sociale zekerheid.

De Registratiekamer heeft in dit kader ook gewezen op de lacune in het structurele toezicht op de uitvoering van de sociale zekerheid. Juist bij gegevensverwerkingen tussen publieke instanties en private partijen is het van belang de rechtmatigheid scherp te bewaken. De toekomstige inspectie Werk en Inkomen, de opvolger van het College van Toezicht Sociale Verzekeringen, controleert slechts het publieke domein. Tot op heden is er geen instantie aangewezen die specifiek tot taak heeft toezicht te houden op de private partijen in de sociale zekerheid. Verantwoorde controle is ook te realiseren

doordat de private partijen hun informatiehuishouding stelselmatig laten onderzoeken door middel van audits. Door kennis te nemen van de resultaten hiervan kunnen hun contractspartners uit de publieke sector en toezichthouders inzicht verkrijgen in de gegevensverwerkingen en zich een oordeel normen over de rechtmatigheid hiervan.

Privatisering arbeidsvoorziening
In het kader van de herstructurering van de sociale zekerheid wordt een deel van de Arbeidsvoorziening verzelfstandigd. Deze nieuwe, private, organisatie, N.V. Kliq, zal in concurrentie met andere reïntegratiebedrijven opdrachten moeten verwerven. De verzelfstandiging gaat gepaard met een overdracht van (persoons)gegevens. In de huidige plannen voor de overgangsregeling is gesteld dat N.V. Kliq eenmalig een kopie krijgt van de gehele database van Arbeidsvoorziening zonder dat deze op maat is gemaakt voor N.V. Kliq. In de database bevinden zich ook persoonsgegevens die niet noodzakelijk zijn voor de uitvoering van de werkzaamheden van N.V. Kliq. De Registratiekamer is van mening dat een dergelijke werkwijze niet getuigt van de vereiste zorgvuldigheid voor de bescherming van persoonsgegevens. Bovendien ontbreekt de grondslag voor een dergelijke verstrekking. Ook moeten betrokkenen op enigerlei wijze worden geïnformeerd over de overdracht van hun gegevens aan een nieuwe organisatie.

Inlichtingenbureau
Een andere nieuwe instantie op het terrein van de sociale zekerheid is het Inlichtingenbureau (IB). Deze instantie faciliteert en stroomlijnt de gegevensuitwisseling tussen de gemeenten en externe inlichtingenbronnen zoals de Belastingdienst en de Informatie Beheer Groep. Aangezien hierdoor vele bestanden gekoppeld worden en vele gevoelige gegevens tussen instanties worden uitgewisseld benadrukt de Registratiekamer ook hier de noodzaak van formele wetgeving, waarin de positie en verantwoordelijkheden van het IB duidelijk zijn vastgelegd. Het IB zal in de toekomst een dermate zelfstandige en centrale rol vervullen dat zij als verantwoordelijke in de zin van de WBP dient te worden aangemerkt.

De structuur van het IB is van groot belang: de handhaving van de regels moet in het informatiesysteem gewaarborgd zijn. Het is niet aan te bevelen deze in te richten als een centrale database waarin alle gegevens worden verzameld: dit leidt namelijk tot onnodige verspreiding van gegevens. In plaats hiervan dient het IB een infrastructuur te zijn die slechts uitwisseling van informatie tussen de decentrale databases van de verschillende instanties mogelijk maakt zonder hierbij gegevens centraal op te slaan of te bewaren. De bescherming van persoonsgegevens is beter gewaarborgd als de gegevensset bij uitwisseling is beperkt tot de meest strikt noodzakelijke informatie, waarbij ook een beperking in de mogelijke beantwoording van vragen (alleen ‘ja’ of ‘nee’) is gewenst. Daar waar een infrastructuur met persoonsgegevens bestaat, zal de roep om verder gebruik van de gegevens vroeg of laat gehoord worden. Ter voorkoming van niet-noodzakelijk verder gebruik van de gegevens dienen de doelstellingen van het IB te worden gespecificeerd en moeten de grenzen van het verenigbaar gebruik worden vastgelegd.

Ontwikkeling van persoonsgebonden nummer in het onderwijs
De tendens naar een uniek persoonsnummer, gebruikt voor meerdere doeleinden, is zichtbaar rondom de invoering van het persoonsgebonden nummer in het onderwijs. Dit nummer zou gebruikt kunnen worden ter controle van het leerlingenaantal op scholen en dienen als beleidsinstrument. De Registratiekamer heeft sterke twijfels geuit bij de noodzaak van de invoering

van een dergelijk persoonsnummer. Haar bezwaren betroffen evenzeer de keuze om hiervoor het sofi-nummer te gebruiken. Het gebruik van dit nummer wordt hiermee uitgebreid naar een nieuwe sector en voor nieuwe doelen. Bovendien wordt het gebruik van het sofi-nummer vervroegd naar de leeftijd van 3½ jaar. Er ontstaat op deze wijze een centraal bestand bij de Informatie Beheer Groep waarin de gehele bevolking in de leeftijd van 3½ tot ongeveer 35 jaar geregistreerd is.

De Registratiekamer heeft zich op het standpunt gesteld dat – als de noodzaak van de invoering van het persoonsgebonden nummer in het onderwijs en van het gebruik van het sofi-nummer daarvoor volgens de wetgever overtuigend is aangetoond – moet worden voorzien in adequate waarborgen die misbruik en oneigenlijk gebruik van de betrokken persoonsgegevens voorkomen en die verdere uitwaaiering van het sofi-nummer kunnen tegengaan. De Registratiekamer constateert met instemming dat uit het wetsvoorstel de ambitie klinkt voor een zorgvuldige en verantwoorde omgang met het sofi-nummer en de daaraan toe te voegen persoonsgegevens. Er is zowel gekozen voor een scheiding van beheer en gebruik als voor een onderscheid tussen gebruik op individueel en niet-individueel niveau. De aandacht voor de waarborgen heeft geresulteerd in een nagenoeg uitputtende wettelijke regeling van de informatievoorziening, wat tevens tegemoet komt aan de eis van transparantie. Deze expliciete wettelijke regelingen stellen hoge eisen aan de naleving en de controle. In welke mate het hoge ambitieniveau in het veld navolging zal vinden, moet worden afgewacht.

Het gebruik van persoonsgegevens door politie en justitie

Verstrekking informatie door Openbaar Ministerie

De roep om het verdere gebruik van persoonsgegevens is ook hoorbaar bij het Openbaar Ministerie (OM). De parketten ontvangen jaarlijks duizenden verzoeken om strafrechtelijke informatie, gedaan door publieke en private organisaties die niet bij het strafproces zijn betrokken. Het gaat hierbij zowel om verzoeken tot verstrekkingen voor doelen die binnen de taakomschrijving van het OM passen, als doelen die daarbuiten vallen. Om te bepalen of deze verstrekkingen in het licht van de WPR en in de toekomst de WBP zijn toegestaan dient eerst te worden vastgesteld of deze wetgeving van toepassing is op persoonsgegevens die gebruikt worden in het kader van het strafproces.

Persoonsgegevens die gebruikt worden in het kader van het strafproces, vallen onder de bepalingen van het Wetboek van Strafvordering (Sv). In de context van het strafproces gelden dus specifieke strafprocessuele regels voor het gebruik van persoonsgegevens. Specifieke regelgeving sluit de algemene regels van de WPR of WBP echter niet uit. De Registratiekamer oordeelde dat ook hier de privacywet van toepassing is. De gegevens in de strafdossiers zijn namelijk te herleiden tot individuele natuurlijke personen. Daarnaast zijn de strafdossiers, in samenhang met het door het OM gebruikte Communicatiesysteem Openbaar Ministerie-Parket Administratie Systeem (Compas), een systematisch aangelegde, samenhangende verzameling. Met deze elementen is voldaan aan de vereisten van het begrip persoonsregistratie en is de WPR van toepassing. Ook de WBP, die betrekking heeft op de verwerking van persoonsgegevens, zal van toepassing zijn op Compas en de daarbij behorende strafdossiers.

De Registratiekamer heeft in het verslagjaar deelgenomen aan het Ontwikkelteam OM en privacy. Dit team had het college van procureurs-generaal ingesteld om de mogelijkheden te onderzoeken voor het verstrekken

van persoonsgegevens door het OM voor buiten het strafproces gelegen doelen. Dit heeft geresulteerd in een uitbreiding van het (model)reglement Compas per 1 mei 2000. Hierin is de recente jurisprudentie van de Raad van State verdisconteerd die een eind maakte aan de selectieve verstrekking van (persoons)gegevens op grond van de Wet openbaarheid van bestuur.

Informatieverplichting door OM

Met het voorgaande hing samen het advies van de Registratiekamer over de invoering van artikel 51g Wetboek van Strafvordering (Sv) dat een wettelijke verplichting creëert op grond waarvan het OM strafrechtelijke gegevens dient te verstrekken aan een derde, indien deze hierbij een gerechtvaardigd belang heeft. De Registratiekamer oordeelde dat dit wetsvoorstel ondeugdelijk is. Het doel van verstrekking, het gerechtvaardigde belang van een derde, valt buiten de taakomschrijving van het OM, zoals vastgelegd in de Wet op de rechterlijke organisatie. Het betreft hier namelijk een buiten de strafrechtspleging en taak van het OM gelegen doel. Deze wettelijke verruiming van de mogelijkheid tot informatieverstrekking kan de toets van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) niet doorstaan.

Uit het EVRM volgt dat informatieverstrekking voor buiten de strafrechtspleging gelegen doelen niet gebaseerd kan worden op een gerechtvaardigd belang van een derde; in dergelijke gevallen dient er een zwaarwegend maatschappelijk belang te zijn. Bovendien zijn strafrechtelijke gegevens bijzondere gegevens waarvoor binnen de WBP een bijzonder regime geldt dat zich verzet tegen de voorgestelde verstrekking door het OM. Naar het oordeel van de Registratiekamer dient de wetgever eerst duidelijkheid te bieden over de reikwijdte van de taak van het OM. Hierna kan worden bezien welke verstrekkingen door het OM aan derden wenselijk zijn en of zij bovengenoemde toetsingen kunnen doorstaan. Een voorziening van verstrekkingen door het OM aan derden in de komende Wet justitiële gegevens is volgens de Registratiekamer het meest aangewezen.

Vorderen informatie voor strafvordering

Technologische ontwikkelingen maken het voor politie en justitie eenvoudiger om aan informatie te komen die noodzakelijk is voor de opsporingstaak. De opsporingsbevoegdheden worden dan ook uitgebreid. Op ruime schaal verlangen de politie en het OM de medewerking van met name het bedrijfsleven bij de opsporing. De gevorderde informatie varieert van dagafschriften van cliënten van banken tot de bonuskaartgegevens van klanten van Albert Heijn. Deze gegevens worden vaak gevorderd op basis van het in het verslagjaar in werking getreden artikel 96a van het Wetboek van strafvordering (Sv). De Registratiekamer heeft hierover klachten vanuit het bedrijfsleven ontvangen en oordeelde dat dergelijke verstrekkingen onrechtmatig zijn.

Artikel 96a Sv is van toepassing op zaken en vermogensrechten en niet op gegevens uit computerbestanden. Voor het onderzoeken en verkrijgen van gegevens uit computerbestanden geeft artikel 125i Sv de rechter-commissaris een specifieke en exclusieve bevoegdheid. Noch de politie noch het OM kan dus op rechtmatige wijze deze gegevens vorderen. Inmiddels heeft ook de minister van Justitie zich uitgesproken tegen de beschreven informatie-inwinning. Indien er geen wettelijke regeling is voor informatieverstrekking, kan de politie slechts om (niet-verplichte) verstrekking verzoeken op basis van artikel 11.2 van de WPR. Dit artikel stelt dat er een dringende en gewichtige reden dient te zijn voor het verzoek. De minister heeft het college van procureurs-generaal verzocht hiervoor een nieuwe gedragslijn uit te werken.

Traceren telecommunicatie
Ook de nieuwe mogelijkheden op telecommunicatiegebied hebben geleid tot uitbreiding van opsporingsbevoegdheden. Zo is een conceptbesluit bij de Telecommunicatiewet (Tw) voorgelegd aan de Registratiekamer. In dit besluit wordt bepaald welke gegevens de aanbieders van mobiele telefonie gedurende drie maanden moeten bewaren en welke gegevens zij moeten verstrekken aan politie, justitie en de Binnenlandse Veiligheidsdienst (BVD). Daarnaast regelt het besluit het gebruik van apparatuur waarmee deze overheidsdiensten de benodigde gegevens zelf uit de lucht kunnen halen (door middel van een zogenaamde IMSI-catchers).

De kritiek van de Registratiekamer betrof onder meer het feit dat niet duidelijk was of de (ruimere) regels rondom het aftappen van telefoons met prepaid cards al dan niet van toepassing zijn op mobiele telefoons met abonnementen. Daarnaast dient te worden aangegeven of bij de gegevensverzameling alleen de medewerking wordt verlangd van de netwerkexploitant of ook van aanbieders van telecommunicatiediensten op het netwerk. Het gebruik van de IMSI-catchers, waarmee de politie verdachte telefoons kan traceren en vervolgens afluisteren, kan leiden tot onbedoelde kennisneming van onverdachte gesprekken. De Registratiekamer vraagt zich af hoe bij het gebruik van deze apparatuur gewaarborgd is dat deze uitsluitend voor de gestelde doelen wordt ingezet. Tevens moet duidelijkheid worden verschaft over de vraag in hoeverre ook de BVD gehouden is aan de eisen rondom het gebruik van IMSI-catchers.

Wetsvoorstel vorderen gegevens telecommunicatie
Een nauw met het voorgaande samenhangend wetsvoorstel zond de minister van Justitie in mei 2000 voor advies toe aan de Registratiekamer, namelijk het concept Wetsvoorstel vorderen gegevens telecommunicatie en het concept Besluit vorderen gegevens telecommunicatie. De voorstellen breiden de bevoegdheden van politie, justitie en de inlichtingendiensten verder uit bij het vorderen van inlichtingen over het telecommunicatieverkeer. Het betreft hier de zogenoemde 'verkeersgegevens': wie belt of internet waar, wanneer en met wie? Daarnaast wordt een duidelijke wettelijke regeling voorgesteld voor het opvragen van nummer, naam, adres en woonplaatsgegevens van abonnees van telecommunicatiediensten.

De Registratiekamer adviseerde tot herziening van de voorstellen. Er moet meer rekening worden gehouden met de toch al verbeterde informatiepositie van de overheid, bijvoorbeeld vanwege het inmiddels op grote schaal voorhanden zijn van historische gegevens over het communicatiegedrag of de beschikbaarheid van locatiegegevens bij mobiele telefonie. De voorziene ongeclausuleerde toegang van inlichtingen- en veiligheidsdiensten tot de gegevens van telecommunicatiebedrijven is disproportioneel.

De overheid zal terughoudender moeten zijn bij het inschakelen van telefoonbedrijven en internetaanbieders vanwege de bijzondere bescherming van het recht op vertrouwelijke communicatie. De reikwijdte van de voorgestelde bepalingen is te onbepaald en daarmee te ruim, de positie van geheimhouders en 'Trusted Third Parties' verdient nadere afweging en er is grote voorzichtigheid geboden bij het verplichten van de sector tot het steeds bewaren van gegevens over het telecommunicatieverkeer voor overheidsdoeleinden. Dat raakt immers ook onverdachte personen.

Het is nodig om een duidelijke wettelijke regeling te maken voor het vorderen van gegevens over de persoon van de gebruiker (gebruikersgegevens). Het gaat

hierbij in verreweg de meeste gevallen om naam- en adresinformatie behorend bij uit printertaps verkregen telefoonnummers en om het verkrijgen van geheime telefoonnummers door politie, justitie en de inlichtingendiensten. De beoogde wettelijke regeling dient te worden getoetst aan artikel 8 van het EVRM en artikel 10 van de Grondwet. Uitgesloten moet worden dat deze bevoegdheid niet kan worden ingezet voor het verdergaande vorderen van verkeersgegevens.

Volgens de Registratiekamer kan voor wat betreft het onderzoek van telecommunicatie door de overheid in zijn algemeenheid als uitgangspunt worden gehanteerd dat telkens de meest vergaande bevoegdheid de mindere omvat. De verplichting tot verstrekking van gebruikersgegevens dient voorts slechts te worden opgelegd aan aanbieders van telecommunicatiediensten en niet aan aanbieders van netwerken, die daarover immers niet de beschikking hebben. Ten slotte verdient de introductie van dwangmiddelen in de fase van het verkennend onderzoek nadere afweging.

Crime in cyberspace

Het grensoverschrijdende karakter van – vooral – computer- of informatiecriminaliteit stelt politie en justitie voor nieuwe vraagstukken. Het noodzaakt nationale instanties tot verdergaande internationale samenwerking op dit terrein. Zo wordt in het kader van de Raad van Europa het zogenaamde 'Cybercrime-verdrag' ontwikkeld, wat ingrijpende gevolgen kan hebben voor de ontwikkeling van het Nederlandse recht. De noodzaak van samenwerking is evident, de Registratiekamer is echter wel van mening dat de bestrijding van deze criminaliteit dient te worden vormgegeven binnen de kaders die een rechtsstaat als de onze past en die zijn geformuleerd in het EVRM.

Het gevaar van verlaging van het niveau van bescherming van grondrechten dreigt indien bevoegdheden van instanties tot aftappen en opnemen van berichtenverkeer en de verplichting tot bewaren en verstrekken van gegevens over het berichtenverkeer verder worden verruimd door nieuwe internationale verdragen. Om disproportionele inbreuken in de communicatievrijheid en de persoonlijke levenssfeer te voorkomen is omzichtigheid geboden. Dit geldt zeker in gevallen waarin wordt samengewerkt met buitenlandse autoriteiten die aan minder strikte regels zijn gebonden. Inbreuken in de communicatievrijheid en de persoonlijke levenssfeer zijn volgens de normen van het EVRM alleen toegestaan indien er aan een aantal stringente voorwaarden is voldaan. Van belang is dat er rekening wordt gehouden met reeds aanwezige strafvorderlijke mogelijkheden. Als er geen aantoonbare noodzaak is dienen de bestaande opsporingsbevoegdheden niet te worden uitgebreid. Een algemene verplichting tot het structureel en langdurig vastleggen van gegevens over communicatieverkeer zal de toets van het EVRM niet kunnen doorstaan. Dergelijke maatregelen staan niet in verhouding tot het doel dat ermee wordt nagestreefd.

Minder ingrijpende maatregelen, zoals een concreet bevel aan een netwerkbeheerder ten aanzien van het vastleggen en verstrekken van gegevens over een specifiek aansluitpunt, hebben eerder de voorkeur. Tevens is transparantie een belangrijke voorwaarde. Dit betekent dat voor vrijwillige medewerking van telecommunicatiebedrijven geen ruimte moet zijn; er dienen duidelijke wettelijke verplichtingen en waarborgen te worden vastgelegd. Het Cybercrime-verdrag dient in dit perspectief tot stand te worden gebracht.

DNA in het strafproces

Technologische ontwikkelingen op een geheel ander terrein, dat van het DNA-onderzoek, maken een verdergaand gebruik van dit lichaamsmateriaal mogelijk. De nieuwe mogelijkheden wakkeren de roep hierom aan. In het verslagjaar zijn twee wetsvoorstellen gedaan die het gebruik van DNA-materiaal bij de opsporing van strafbare feiten mogelijk maken.

Beperkt gebruik DNA-materiaal

Het DNA-profiel, ofwel een 'digitale vingerafdruk', is te vergelijken met een echte vingerafdruk; het bevat slechts een beperkt aantal gegevens. Hiervoor is gebruik gemaakt van het DNA-celmateriaal. Het celmateriaal bevat echter veel meer informatie: hierin liggen in beginsel alle erfelijke eigenschappen van een individu besloten. Verdergaand gebruik zou kunnen leiden tot een daderprofiel dat informatie bevat over het signalement van de betrokkene. Deze mogelijkheid wordt een steeds grotere realiteit.

In het ontwerpbesluit DNA-onderzoek in strafzaken benadrukte de minister van Justitie dat celmateriaal alleen mag worden afgenomen, gebruikt en bewaard voor het vervaardigen van DNA-profielen en niet voor andere doeleinden zoals het achterhalen van erfelijke eigenschappen of ziekten. De Registratiekamer onderschreef dit standpunt en adviseerde om het gebruik van DNA-onderzoek en DNA-profielen uitdrukkelijk wettelijk te begrenzen. Dit dient ook te geschieden door het bewaren van celmateriaal tot een minimum te beperken. Het celmateriaal zou in beginsel vernietigd moeten worden zodra het vonnis definitief is.

Indien er tot opslag van DNA-celmateriaal, zowel afgenomen bij verdachten als gevonden in sporenmateriaal, wordt besloten, betekent dit het begin van een biometrische databank. Deze zal gestaag groeien met de uitbreiding van de kring van mensen die materiaal afstaan. Naarmate uit het materiaal in de toekomst meer informatie kan worden afgeleid, wordt deze databank een basisregistratie van een groeiend aantal persoonskenmerken van een groeiend aantal mensen. Dit roept vele prangende problemen op. Hoe wordt omgegaan met nieuwe technologische mogelijkheden? Hoe wordt het DNA-celmateriaal verder gebruikt? De Registratiekamer vraagt zich af of de draagwijdte van deze ontwikkeling voldoende wordt onderkend.

Vaststellen uiterlijke persoonskenmerken

Niet in overeenstemming met de restrictieve opstelling van de minister van Justitie achtte de Registratiekamer het wetsontwerp dat een wettelijk kader creëert voor het vaststellen van uiterlijke persoonskenmerken aan de hand van celmateriaal, in het kader van de opsporing en vervolging van strafbare feiten. In dit stadium acht de Registratiekamer het ontwerpen van een dergelijk juridisch raamwerk voor verdergaande toepassing prematuur. De maatschappelijke discussie over de ethische grenzen van het gebruik van celmateriaal is nog niet gevoerd. Het maatschappelijk debat is noodzakelijk voor het vaststellen van de contouren van het maatschappelijk verantwoord gebruik van DNA-celmateriaal. Daarna kan wetgeving volgen. In het voorgelegde voorstel is al een voorschot genomen op de mogelijke uitkomst van het debat.

Gedragscodes

De Registratiekamer bevordert als tweedelijnsorganisatie zelfregulering in de maatschappelijke sectoren. In dit kader heeft zij tot taak de totstandkoming van privacygedragscodes te stimuleren en de kwaliteit ervan door middel van een

vrijwillige goedkeuringsprocedure te toetsen. Zij is dan ook verheugd te constateren dat in een aantal sectoren waarin persoonsgegevens een belangrijke plaats innemen, wordt gewerkt aan het opstellen van gedragscodes die van toepassing zullen zijn onder de WBP. Onder anderen in de financiële sector, de direct-marketingbranche en de farmaceutische industrie staat de invoering van privacygedragscodes op de agenda. Andere sectoren wachten met het indienen van nieuwe gedragscodes tot de inwerkingtreding van de WBP. De Registratiekamer is in het verslagjaar wel met diverse brancheorganisaties in overleg geweest over de totstandkoming ervan.

Banken en verzekeraars

De Nederlandse Vereniging van Banken heeft in het verslagjaar overleg gevoerd met de Registratiekamer over de invoering van een nieuwe, WBP-conforme, privacygedragscode. De verklaring van overeenstemming met de gedragscode van het Verbond van Verzekeraars loopt in 2001 af. Daarom is ook het Verbond van Verzekeraars in gesprek met de Registratiekamer over vernieuwing van de privacycode. De Registratiekamer is tevens betrokken bij de opstelling van een addendum bij deze code van Zorgverzekeraars Nederland, die specifiek aandacht heeft voor het speciale regime rond medische persoonsgegevens.

Andere Nederlandse codes

De gedragscode van de brancheorganisatie van de farmaceutische industrie, Nefarma, is verlengd tot de inwerkingtreding van de WBP. Zodra de wet van kracht is zal een bijgewerkte code aan de Registratiekamer worden voorgelegd. Er heeft in het verslagjaar overleg plaatsgevonden over de conceptgedragscode van de Nederlandse Vereniging van Handelsinformatiebureaus, die eerder aan de Registratiekamer was voorgelegd. Deze code zal in 2001 nader worden uitgewerkt. De automobielbranche, vertegenwoordigd in de RDC, heeft in 2000 een concept gemaakt voor een privacygedragscode en zal deze voorleggen aan de Registratiekamer als de nieuwe wet in werking treedt.

Europese codes

De Europese privacyrichtlijn, richtlijn 95/46/EG, biedt de mogelijkheid tot het ontwerpen van privacygedragscodes die van kracht zijn in de gehele Europese Unie. Deze codes worden ter goedkeuring voorgelegd aan de ‘artikel 29’ werkgroep, de onafhankelijke raadgevende vergadering van de Europese toezichthouders. De werkgroep heeft regels opgesteld waaraan de Europese codes moeten voldoen. Enkele Europese brancheorganisaties hebben tot nu toe van deze mogelijkheid gebruik gemaakt. In het verslagjaar heeft de werkgroep overleg gevoerd met de FEDMA, de Europese brancheorganisatie voor direct-marketingbedrijven, over een concept privacycode. De verwachting is dat deze code in de loop van 2001 goedgekeurd zal worden. De Europese farmaceutische industrie, georganiseerd in de EFPIA, heeft gewerkt aan het opstellen van een Europese gedragscode die naar alle waarschijnlijkheid in een later stadium aan de werkgroep zal worden voorgelegd. Ook met de IATA, de organisatie van luchtvaartmaatschappijen, zijn gesprekken gevoerd over de mogelijke ontwikkeling van een Europese privacycode.

Normatieve kaders

Bij het uitoefenen van haar taken signaleert de Registratiekamer regelmatig dat er in de maatschappij behoefte bestaat aan meer duidelijkheid over de omgang met persoonsgegevens in concrete situaties. Ook in andere publicaties geeft de Registratiekamer invulling aan de voor een specifiek onderwerp relevante privacyregels.

In het verslagjaar heeft de Registratiekamer onderzoek gedaan naar de omgang met persoonsgegevens door internetserviceproviders, de normen voor etnomarketing en de gevolgen voor de verwerking van persoonsgegevens van de ontwikkelingen in de bank- en verzekeringswereld. Ook besteedde zij aandacht aan de privacyregels voor creditscoring en heeft zij in een studie vuistregels vastgelegd voor het internet- en emailgebruik op de werkplek. In haar onderzoeksrapporten is de Registratiekamer onder andere ingegaan op screening door de politie, de zorg voor gegevens bij indicatiestelling en het verstrekken van gegevens door de belastingdienst. Deze onderzoeken zijn gedaan in het licht van de WBP en bieden daarmee een houvast voor de betrokken sectoren als deze wet in 2001 in werking treedt. In hoofdstuk 1 is nader ingegaan op de inhoud van deze rapporten

Geschillen voorkomen en beslechten

Op het grensvlak van normontwikkeling en handhaving ligt de betrokkenheid van de Registratiekamer bij geschillen. Het kan gaan om de behandeling van klachten of verzoeken om bemiddeling. Ook kan in een voorstadium advies worden gevraagd, juist om geschillen te voorkomen. In dit bestek volgen enkele casus die betrekking hebben op het rechtmatig gebruik van persoonsgegevens in verschillende relaties. Vooraf gaat de kwestie van de hielprik, waarbij de toepasselijkheid van de wetgeving in het geding was.

Persoonsgegeven/persoonsregistratie

Van een persoonsgegeven is sprake als een gegeven informatie verschaft over een identificeerbare (natuurlijke) persoon. Voor de toepasselijkheid van de wet is wel vereist dat het gaat om persoonsgegevens die deel uitmaken van een persoonsregistratie.

Kort na de vuurwerkramp in Enschede op 13 mei 2000 is gesuggereerd dat het bloed dat bij nagenoeg alle pasgeboren baby's wordt afgenomen en opgeslagen bij het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) gebruikt kan worden voor identificatie van slachtoffers via DNA-analyse. Over de rechtmatigheid van het bewaren van de bloedmonsters zonder de ouders daarover tevoren te informeren, laat staan om toestemming te vragen rezen vragen in pers en politiek.

De Registratiekamer stelde een onderzoek in waarbij zij eerst de vraag moest beantwoorden of de Wet persoonsregistraties (WPR) van toepassing was op de opslag van de bloedmonsters. De Registratiekamer kwam tot het oordeel dat het bloed als zodanig niet als een persoonsgegeven is aan te merken, maar wel als de bron van persoonsgegevens kan worden beschouwd. Het RIVM is in staat om uit het bloed bepaalde gegevens te verkrijgen. Overigens stelde de Registratiekamer op grond van een onderzoek ter plaatse vast dat de WPR niet van toepassing was, omdat de dozen met de verzameling bloedmonsters niet een dermate gestructureerde verzameling gegevens vormden dat sprake was van een persoonsregistratie.

De Registratiekamer heeft als maatschappelijke taak constructief bij te dragen aan de bescherming van de persoonlijke levenssfeer in het algemeen. Op grond daarvan heeft zij geadviseerd aan het RIVM en de ministers van Volksgezondheid, Welzijn en Sport (VWS) en Justitie de volgende maatregelen te treffen:

- ouders over de opslag van hielprikbloed informeren en ten minste de mogelijkheid bieden om bezwaar te maken;
- de mogelijkheid onderzoeken van expliciete wetgeving met het oog op toekomstige risico's bij de opslag van lichaamsmateriaal;

– het scheppen van meer rechtszekerheid over de toepasselijkheid van beroepsgeheim en verschoningsrecht;
– het realiseren van een adequaat toezicht.

In de loop van 2000 heeft de minister van VWS de Tweede Kamer laten weten dat zij gevolg zal geven aan de aanbevelingen uit het rapport.

Rechtmatig gebruik

Divers zijn de vragen die de Registratiekamer krijgt voorgelegd naar de rechtmatigheid van het gebruik van persoonsgegevens voor andere doeleinden dan waarvoor deze zijn verkregen. Deze vraag is naar huidig en komend recht één van de meest cruciale voor de normering van het gebruik van persoonsgegevens. Bij de beschrijving van deze kwesties is een onderscheid gemaakt naar de relatie waarin de geregistreerde staat tot de organisatie of het bedrijf dat zijn persoonsgegevens verwerkt. Zo komen achtereenvolgens de geregistreerde als burger, klant, werknemer, patiënt, verzekerde en combinaties daarvan aan de orde.

De geregistreerde als burger

Twee situaties betreffen het verstrekken van persoonsgegevens aan gemeenten in verband met het controleren of de betrokkenen al dan niet als inwoner moesten worden aangemerkt. In de eerste casus ging dit om subsidieverlening; de tweede situatie betrof de vraag of recreatiewoningen voor permanente bewoning worden gebruikt.

Een gemeente moet waken voor een juiste besteding van subsidiegelden. Daarom vragen gemeenten ledenlijsten van verenigingen op, die subsidie krijgen. In de gemeenteraad van Zaandam werden vragen gesteld over de rechtsgeldigheid van dit controlemiddel. Op de ledenlijst staan immers gegevens van individuele personen en de vraag is gerezen of dit niet in strijd komt met de privacywetgeving.

De eerste vraag is of deze verstrekking voortvloeit uit het doel van de vereniging. De Registratiekamer oordeelde dat doorgaans verstrekking van gegevens over leden aan buitenstaanders niet als een doel van de ledenadministratie is aan te merken. Ook een administratie van deelnemers aan bepaalde activiteiten, zoals cursussen, zal in de regel slechts dienstbaar zijn aan een goed verloop van die activiteiten en het verkeer tussen de betrokken deelnemers.

Evenmin is sprake van een wettelijk voorschrift als grondslag voor de verstrekking van gegevens aan de gemeente. Zo'n voorschrift dient voldoende nauwkeurig te zijn en ook adequate en effectieve waarborgen te bevatten tegen ongeoorloofde inbreuken. De Algemene wet bestuursrecht bevat een voorschrift dat bij subsidieverlening de gegevens moeten worden verschaft die nodig zijn voor de beslissing op de aanvraag. Maar artikel 4.3 van deze wet schept ook een belangrijke waarborg tegen het opleggen van te vergaande verplichtingen. Deze mogen namelijk niet zover gaan dat het belang daarvan niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer. Deze afweging kan ook geschieden door de wetgever die uitdrukkelijk verplicht tot het overleggen van bepaalde gegevens.

Wat betekent dit nu voor de situatie in de gemeente Zaandam? Deze heeft als criterium voor de subsidietoewijzing bepaald dat een minimaal aantal leden of deelnemers woonachtig is in de gemeente. Met het oog daarop gebruikt de gemeente een standaardformulier waarop zij gegevens vraagt over het aantal in

Zaandam woonachtige personen. Zij verzoekt om bijvoeging van de ledenlijst en behoudt zich het recht voor deze te controleren.

De Registratiekamer acht deze algemene verplichting om een leden- of deelnemerslijst te overleggen een onevenredige inbreuk op de persoonlijke levenssfeer van die leden of deelnemers. Het legitieme belang van het gemeentebestuur om een voldoende nauwe band met de gemeente te waarborgen zal op een andere, voor de privacy van betrokkenen minder ingrijpende, wijze bereikt kunnen worden. Daarbij valt in het bijzonder te denken aan controle op basis van steekproeven, al dan niet door een onafhankelijke derde. Ook het vragen van toestemming aan de leden is geen reële optie. Uit het voorgaande vloeit immers voort dat de noodzaak voor de verstrekking en daarop volgende registratie door de gemeente onvoldoende is onderbouwd.

De privacywetgeving stelt ook grenzen aan de bevoegdheid van gemeenten om te controleren of personen permanent in de gemeente wonen of daar slechts recreatief verblijven. Recreatiegemeenten proberen al jaren permanente bewoning van recreatiewoningen tegen te gaan. De gemeente Ede legde de Registratiekamer haar plannen voor gegevens over de bewoners van recreatiewoningen op te vragen bij diverse instellingen en diensten. Door het verzamelen van deze gegevens zou de gemeente aanwijzingen kunnen verkrijgen dat mensen een recreatiewoning permanent bewonen. Het gaat om de volgende informatiebronnen: Kamer van Koophandel, Rijksbelastingen, Gemeentelijke basisadministratie, gemeentelijke belastingadministratie, kadaster- en hypotheekregister, postbussenbestand, administraties van andere gemeenten, milieuheffingenadministratie van het waterschap, energiebedrijf, ziekenfonds, woningbouwverenigingen en -stichtingen, leerplichtregistratie en de kentekenregistratie in Veendam. De vraag was in hoeverre deze praktijk op bezwaren stuit vanuit de privacywetgeving.

De Registratiekamer stelde voorop dat het onbeperkt gegevens verzamelen niet mogelijk is, want wonen of recreatief verblijven is een privacygevoelige activiteit. Met de controle en de daaraan gekoppelde gegevensuitwisseling kan dus een aanzienlijke inbreuk op de persoonlijke levenssfeer gepaard gaan. Het uitvoeren van onderzoeken en het opvragen en vastleggen van persoonsgegevens mag alleen plaatsvinden als aangetoond kan worden dat andere voorzieningen niet mogelijk of effectief zijn. In een zo vroeg mogelijk stadium moeten daarom ook maatregelen worden genomen, waardoor de permanente bewoning wordt voorkomen of bewijsbaar gemaakt voor de gemeente.

De Registratiekamer stelde vast dat er niet is voorzien in een specifieke wettelijke bevoegdheid voor het verzamelen van informatie. Wel kan het overtreden van voorschriften die deel uitmaken van een bestemmingsplan ingevolge de Wet op de ruimtelijke ordening een strafbaar feit opleveren. Maar dan is al snel sprake van een opsporingsonderzoek. Gemeenteambtenaren mogen in dat kader geen opsporingsactiviteiten verrichten. Zaken die daartoe aanleiding geven, moeten dan ook overgedragen worden aan opsporingsambtenaren.

De Registratiekamer beveelt de gemeente aan om de gevallen waarin er een indicatie of een vermoeden van onterechte permanente bewoning is ontstaan, zorgvuldig te selecteren. De indicatoren die kunnen leiden tot een vermoeden moeten daarbij helder en scherp worden gesteld. Dat leidt tot een doeltreffende

selectie en het voorkomen van onnodige gegevensverzameling. Er dient een rangorde in de gegevensbronnen aangehouden te worden. Het verdient aanbeveling eerst bij de betrokkene te informeren, voordat andere bronnen worden geraadpleegd. In het algemeen dient eerder uit interne dan uit externe gegevensbronnen te worden geput. Controle dient primair geconcentreerd te zijn op de inschrijving in de Gemeentelijke basisadministratie.

Voor gebruik van gegevens uit de gemeentelijke belastingadministratie moet de gemeenteraad bij raadsverordening ontheffing van de geheimhoudingsplicht verlenen. Verder is het de verantwoordelijkheid van de houder van de registratie waaruit gegevens verstrekt zouden moeten worden, om te beslissen of een verstrekking aan de gemeente plaats zal vinden. Er is geen verplichting, maar hooguit een bevoegdheid om te verstrekken. Het gaat daarbij om een beslissing waarbij de concrete omstandigheden moeten worden meegewogen, en die wordt genomen na toetsing aan het voor de verstrekkende instantie geldende verstrekkingenregime. De betrokken instanties moeten in hun beslissing laten meewegen de mate waarin de gemeente aan de voorwaarden voor zorgvuldige verwerking van persoonsgegevens voldoet.

In de Tweede Kamer is inmiddels een motie aanvaard die beoogt het instrumentarium van gemeenten uit te breiden. Gemeentebesturen zouden thans onvoldoende doeltreffende instrumenten ter beschikking hebben om permanente bewoning van recreatiewoningen te voorkomen of te bestrijden.

De geregistreerde als klant

Het staat een bedrijf niet vrij om zomaar zijn klantgegevens aan andere bedrijven te verstrekken. Hiervan worden drie voorbeelden gegeven: de ANWB aan een creditcardmaatschappij, een telecomaanbieder aan de uitgever van een telefoongids en een autodealer aan zijn importeur.

Sommige ANWB-leden hadden een opgewaardeerde lidmaatschapskaart voor het betalen van parkeergeld. Die lidmaatschapskaart is vervangen door een creditcard. De ANWB heeft daarvoor de gegevens van de kaartbezitters doorgegeven aan de creditcardmaatschappij die vervolgens een kredietwaardigheidtoets bij het Bureau Kredietregistratie (BKR) in Tiel heeft uitgevoerd. De Registratiekamer ontving hierover klachten en stelde een onderzoek in.

De ANWB stelde dat zij de persoonsgegevens mocht verstrekken, aangezien de verstrekking voortvloeit uit haar doelstelling: het aanbieden van activiteiten ten behoeve van de uitbreiding van het ledenbestand en afzet van producten en diensten. Het gaat hierbij om een ‘koepeldoelstelling’. Bij de toepassing van zo’n ruime doelstelling in een bepaalde situatie moet gelet worden op die onderdelen van de doelstelling die daarvoor specifiek van belang zijn.

De centrale vraag is daarom niet of de gegevensverstrekking voortvloeit uit het door de ANWB geformuleerde algemene doel, maar of de gegevensverstrekking voorvloeit uit het specifieke doel waarvoor de betreffende gegevens zijn verzameld: in dit geval het uitvoeren van de ‘parkeer-betaal’ overeenkomst met haar leden. De nieuwe betaalfaciliteit kent grote verschillen met de oude opgewaardeerde lidmaatschapspas. Een creditcard biedt namelijk behalve het betalen van parkeergeld vele andere mogelijkheden; de geboden faciliteit is veel ruimer dan de dienst waarvoor de gegevens zijn verzameld. Bovendien moet rekening worden gehouden met de consequenties van de gegevensverzameling voor de privacybelangen van de geregistreerden, zoals de BKR-toets, voor veel

mensen een onderzoek met een gevoelig karakter. De Registratiekamer kwam dan ook tot de conclusie dat de ANWB tenminste een bezwaarmogelijkheid had moeten bieden aan zijn klanten. Alleen zo had de ANWB voldoende rekening gehouden met de belangen van de betrokkenen. Nu dit niet gebeurd is, had de gegevensverstrekking door de ANWB aan een creditcardmaatschappij niet op deze manier mogen plaatsvinden.

Een aanbieder van mobiele telefonie vroeg of hij de abonneegegevens, naam-, adres- en woonplaats- (NAW) gegevens en mobiele telefoonnummers, mag verstrekken aan de uitgever van een universele telefoongids. Er waren tevoren hierover geen afspraken gemaakt met de abonnees. De Registratiekamer toetste deze vraag aan de criteria voor het verenigbaar gebruik van persoonsgegevens uit artikel 9 van de Wet bescherming persoonsgegevens. De door het bedrijf voorgestelde procedure waarbij de abonnees bezwaar kunnen maken tegen verstrekking bood volgens haar onvoldoende waarborgen. Zij adviseerde het bedrijf zijn abonnees verschillende opties voor te leggen, die artikel 11.6 van de Telecommunicatiewet biedt. Daarbij valt te denken aan de mogelijkheid om helemaal niet in de gids vermeld te worden of slechts met de gegevens die voor de gids noodzakelijk zijn.

Een autodealer wordt door zijn importeur verplicht NAW-gegevens van zijn klanten aan de importeur door te geven bij het bestellen van een auto. Deze verplichting is opgenomen in de overeenkomst tussen de dealer en de importeur. Bij niet-nakoming van deze verplichting kan de importeur weigeren auto's aan de dealer te leveren. De Registratiekamer onderzocht deze zaak. De BOVAG liet weten een toenemende behoefte aan marketing die is afgestemd op de levensstijl van de klant, te verwachten. De BOVAG wijst het vragen van gegevens door importeurs af, als die verder gaan dan noodzakelijk is voor de afhandeling van claims in verband met fabrieksgarantie of het gebruikmaken van een Europees hulpnet.

De Registratiekamer overwoog dat het verstrekken van klantgegevens door de dealer dient voort te vloeien uit het doel van zijn registratie. Dat betekent dat gegevens mogen worden verstrekt als de rechtsverhouding daartoe aanleiding geeft. Van een rechtsverhouding tussen de klant en de importeur zal slechts in uitzonderingssituaties sprake zijn. Het is dan ook niet aannemelijk dat de importeur een redelijk belang heeft bij het aanleggen van een database met klantgegevens voor distributiedoeleinden. Het is immers zeer wel mogelijk om op grond van het aantal bestellingen de productiecapaciteit te verdelen zonder dat de importeur behoeft te vernemen wie de klant is.

De importeur kan wel een aparte taak hebben op het gebied van zogenaamde serviceondersteuning voor het automerk. Het gaat daarbij om taken die aanvullend of ondersteunend zijn ten opzichte van de overeenkomst tussen klant en dealer, zoals garantieverplichtingen, onderhoudsondersteuning en rechtstreekse communicatie over onvoorziene levertijd. Hiertoe kan de dealer dan ook gegevens aan de importeur verstrekken.

Voor het uitvoeren van "recalls" en direct marketingactiviteiten kan de importeur ook gegevens verkrijgen van het RDC. Houders van kentekens hebben krachtens de Wegenverkeerswet 1994 een blokkeringsrecht voor commercieel gebruik van kentekengegevens door de automobielbranche. Een blokkering wordt aangetekend bij de RDW en het RDC. Dit recht mag door de importeur niet worden omzeild door gegevens te verkrijgen bij de dealer. Voor alle andere verstrekkingen door de dealer aan de importeur is de toestemming van de betrokkenen vereist.

De geregistreerde als klant en werknemer
De vraag is voorgelegd of een telecombedrijf zonder toestemming van de werknemer gespecificeerde telefoonnota's aan zijn werkgever mag sturen, indien deze betaalt voor de aansluiting. De klacht betrof een werknemer die met zijn privé-telefoon veel voor zijn werk belde. Zijn baas nam daarom alle gespreks- en abonnementskosten voor zijn rekening. De werknemer ontving niet-gespecificeerde nota's en hij verzocht het telefoniebedrijf deze nota's naar zijn werkgever te sturen. Deze verzocht daarop om toezending van gespecificeerde nota's. Het bedrijf voldeed aan dit verzoek. De werknemer was hiervan noch door zijn werkgever noch door het bedrijf op de hoogte gesteld. Het telefoniebedrijf stelde zich op het standpunt dat de werkgever als de vertegenwoordiger van de werknemer was te beschouwen en dat de verstrekking daarom was toegestaan.

De Registratiekamer kwam tot het oordeel dat het telefoniebedrijf niet zonder toestemming van de werknemer een gespecificeerde nota aan diens werkgever had mogen sturen. Het betalen van iemands telefoonnota kan inderdaad gezien worden een vorm van vertegenwoordiging. Het telefoonbedrijf heeft echter geen reden om aan te nemen dat deze vertegenwoordiging zich ook uitstrekt tot het inwinnen van nadere gegevens over de nota. Daarbij speelt een rol dat werkgevers en werknemers tegengestelde belangen kunnen hebben. De Registratiekamer beveelt het telefoniebedrijf aan om de abonnees die hun nota naar iemand anders laten sturen, erop te wijzen dat deze persoon buiten hen om een gespecificeerde nota kan krijgen. Ook moet het telefoniebedrijf deze abonnees de mogelijkheid bieden dat dat alleen gebeurt met hun toestemming, of dat de gespecificeerde nota's alleen naar hun eigen adres worden verstuurd.

De geregistreerde als klant en patiënt
Een ziekenhuis attendeerde de Registratiekamer op de verplichting die de minister van VWS de hartcentra oplegde informatie over patiënten te verstrekken aan fabrikanten van hartkleppen. De minister wilde op deze wijze komen tot een 'post marketing surveillance systeem' waarmee fabrikanten het functioneren van de hartkleppen van patiënten kunnen volgen.

De Registratiekamer constateerde een mogelijke schending van het medisch beroepsgeheim en de privacywetgeving. In overleg met het ministerie is de volgende werkwijze afgesproken: elk ziekenhuis houdt zelf bij welke patiënt welke hartklep heeft gekregen. De fabrikant houdt bij welke hartkleppen aan welk ziekenhuis zijn verkocht. In geval van een calamiteit informeert de fabrikant het ziekenhuis over de serienummers waar een probleem mee is. Het ziekenhuis informeert de patiënt. Wanneer een ziekenhuis een calamiteit ontdekt, meldt deze dat aan de fabrikant en de Inspectie voor de Gezondheidszorg, zodat alle betrokken ziekenhuizen op de hoogte gesteld kunnen worden.

De geregistreerde als patiënt en verzekerde
Een steeds terugkerend aandachtspunt is de uitwisseling van medische gegevens bij de uitvoering van (zorg)verzekeringen. Het vermelden waard zijn de verstrekking door een zorgverzekeraar van gegevens aan een leverancier van voeding, de verstrekking door een thuiszorginstelling aan een indicatieorgaan en verstrekkingen van medische gegevens aan een assurantietussenpersoon

Een zorgverzekeraar heeft gegevens van ziekenfondsverzekerden die in aanmerking komen voor vergoeding van voeding, verstrekt aan een leverancier van voeding. Een verzekerde heeft hierover bij de Registratiekamer geklaagd.

De Registratiekamer stelde vast dat de verzekerde op grond van de Ziekenfondswet aanspraak heeft op een vergoeding in natura. Dit houdt in dat zorgverzekeraar de vergoeding niet in geld verstrekt maar in natura, in dit geval voeding. De zorgverzekeraar heeft met één leverancier van voeding een overeenkomst gesloten. Hierdoor kan deze leverancier voeding aan ziekenfondsverzekerden leveren. De zorgverzekeraar heeft voor het verstrekken van de vergoeding in natura een machtiging verleend aan de leverancier. Om deze machtiging uit te voeren is het noodzakelijk dat de leverancier beschikt over relevante gegevens van de verzekerde. Met het oog hierop mag de zorgverzekeraar dus gegevens van verzekerden verstrekken aan de leverancier. De Registratiekamer heeft in haar oordeel meegewogen dat de zorgverzekeraar de verzekerde schriftelijk op de hoogte heeft gesteld dat de leverancier de voeding gaat leveren.

Bij de Registratiekamer is geklaagd over de verstrekking van gegevens door een thuiszorginstelling zonder toestemming van betrokkene aan een Regionaal Indicatie Orgaan (RIO). Deze gegevens waren nodig voor het stellen van een herindicatie voor de thuiszorg. In het privacyreglement van de thuiszorginstelling is aangegeven dat verstrekking van gegevens aan derden, zoals een RIO, alleen plaatsvindt op basis van toestemming, tenzij een wettelijke regel die verstrekking dwingend voorschrijft. Dit zou het Zorgindicatiebesluit kunnen zijn, maar daarin is nu juist bepaald dat gegevens slechts mogen worden gebruikt voor de indicatiestelling met toestemming van de zorgvrager. Dus is de bestreden verstrekking niet toegestaan.

Een verzekerde verzocht zijn verzekeringsmaatschappij om premievrijstelling van zijn hypotheekverzekering. In de aanvraag zijn gegevens over de gezondheid van de verzekerde opgenomen, met name de aard van de ziekte, ziekenhuisopname en gebruikte medicijnen. De verzekerde stuurde het formulier in via een assurantietussenpersoon. De verzekeringsmaatschappij wijst de aanvraag af. De afwijzingsbrief met daarin informatie over de achtergrond van de ziekte wordt hem zonder enige afscherming toegestuurd via de assurantietussenpersoon. De verzekerde klaagt hierover bij de Registratiekamer.

De verzekeringsmaatschappij stelde dat de assurantietussenpersoon gezien moet worden als vertegenwoordiger van de verzekerde en dat de verstrekking daarom niet was aan te merken als een verstrekking aan derden. De Registratiekamer kon er zich in vinden dat de assurantietussenpersoon als adviseur en belangenbehartiger van de verzekerde wordt beschouwd, maar daarmee nog niet als diens vertegenwoordiger in juridische zin kan worden aangemerkt. Dat hij de formulieren via de tussenpersoon verzendt verandert hier niets aan.

Gegevensverstrekking aan de tussenpersoon van de verzekerde is dan ook aan te merken als een verstrekking aan derden. Omdat het in dit geval gaat om gegevens die verstrekt zijn door de medisch adviseur van een verzekeringsmaatschappij, zijn ook de beroepsregels die gelden voor verzekeringsartsen van belang. De verzekeringsbranche heeft de regels uit de WPR en die beroepsregels verwerkt in een gedragscode. Gegevensverstrekking door een verzekeringsmaatschappij aan de tussenpersoon van een verzekerde zal in het algemeen wel uit het doel van de registratie voortvloeien. Als het gaat om gegevens in verband met een keuring staat de zwijgplicht van de verzekeringsarts dat echter niet toe. De tussenpersoon behoort namelijk niet tot degenen aan wie de verzekeringsarts in verband met zijn werkzaamheden

gegevens kan verstrekken. Voor deze verstrekking is dus toestemming van de verzekerde nodig. De toestemming hoeft niet schriftelijk te worden gegeven maar moet wel uit iets blijken.

Dat de verzekeringsmaatschappij in dit geval heeft aangenomen dat de verzekerde toestemming had gegeven om ook correspondentie waarin gegevens van de medisch adviseur waren opgenomen, via de tussenpersoon te verzenden is niet onbegrijpelijk. Het is immers heel gebruikelijk dat correspondentie met een verzekerde via zijn tussenpersoon wordt gevoerd. In dit geval had de verzekerde zelf al eerder gegevens over zijn gezondheid verstuurd zonder die voor de tussenpersoon af te schermen. Om echter van toestemming te kunnen spreken, had de verzekerde de beschikking moeten hebben over voldoende informatie om zijn standpunt over de gegevensverstrekking te bepalen. Dat was niet het geval. De plicht om die informatie te geven ligt bij de verzekeringsmaatschappij en de medisch adviseur. De in dit geval gevolgde werkwijze staat dan ook op gespannen voet met de beroepsregels voor verzekeringsartsen en met de Gedragscode verwerking persoonsgegevens verzekeringsbedrijf.

Een andere kwestie raakt de assurantietussenpersoon die in dienst is van een verzekeringsmaatschappij. Ook hier speelde de vraag of deze 'loondienstagent' kennis kan nemen van gegevens over de gezondheid die zijn verstrekt in verband met het aangaan of uitvoeren van een verzekeringsovereenkomst.

De Registratiekamer kwam tot het oordeel dat de WBP verwerking van gezondheidsgegevens door de loondienstagent onder bepaalde voorwaarden toelaat. Zo is de verwerking mogelijk als die plaatsvindt in het kader van de risicobeoordeling én de betrokkene geen bezwaar heeft gemaakt. De loondienstagent zal betrokkene dus vóór het moment van verzamelen, bijvoorbeeld bij het uitreiken of toezenden van de gezondheidsverklaring, moeten informeren over de mogelijkheid om bezwaar te maken. Dat betekent in de praktijk dat de (aspirant)verzekerde de verklaring ook in gesloten enveloppe rechtstreeks aan de medisch adviseur moet kunnen toezenden.

Daarnaast kan de medisch adviseur zonder expliciete toestemming van de verzekerde gegevens verstrekken aan degenen die noodzakelijkerwijs bij zijn werkzaamheden betrokken zijn. Dit betekent dat als de loondienstagent onder verantwoordelijkheid van de medisch adviseur kennis neemt van de gegevens van de aspirant-verzekerde die voor een goede vervulling van zijn taak nodig zijn, dit niet in strijd komt met het beroepsgeheim van de medisch adviseur.

Technologie

Computerprogramma's die jaartallen van twee cijfers niet juist konden interpreteren, veroorzaakten het millenniumprobleem. Nu dit probleem is opgelost, wordt het grote aanbod aan ICT- en internettoepassingen nog duidelijker. De nieuwe digitale wereldeconomie leidt tot een ongebreidelde toegang tot informatie en kennis, het elimineren van afstanden, het onbelangrijk worden van één bepaalde fysieke locatie voor actor, actie en gevolgen van die actie en tot het comprimeren van tijd. Er is ook sprake van globalisering bij multinationals die waar ook ter wereld direct met hun medewerkers, commerciële partners, klanten, aanbieders en afnemers verbonden zijn.

In de telecommunicatiemarkt is een andere trend zichtbaar: er wordt in een hoog tempo wereldwijd geliberaliseerd waardoor (staats)monopolies op telecommunicatiegebied verdwijnen. Mobiele telefonie verdringt de vaste-lijnverbindingen. Er gaan nu al meer data dan dat er spraak over de lijn gaat. Innovatie, concurrentie en lagere transmissiekosten leiden tot sterke prijsdalingen. Die lagere prijzen leiden tot meer vraag van de burger/consument, niet alleen naar telefonie maar vooral ook naar data, beeld en geluid. De internetexplosie laat dan ook een sterk toenemende groei van gebruikers zien: de afgelopen jaren was de gemiddelde groei wereldwijd 25% per jaar.

Technologiefondsen zijn op de beurzen snel in waarde gestegen, maar even opvallend weer in waarde gedaald. Beursintroducties zijn mislukt. Er is daardoor enige stagnatie in de ontwikkeling van de nieuwe economie opgetreden.

Desondanks hebben deze ontwikkelingen grote gevolgen voor de burger, in zijn rol van klant, afnemer of consument. Het gehele marketingarsenaal is gericht op het volledig transparant maken van de consument en het binden van de klant aan de aanbieder van om het even welke goederen of diensten. Zijn voorkeuren, gedrag en fysieke verplaatsingen zullen van minuut tot minuut gevolgd worden door het gebruik van geavanceerde analyse- en marketinggereedschappen, zoals data warehousing en data mining.

Voor de gebruiker van internet is het moeilijk om na te gaan welke informatie over hem is opgeslagen. Wordt hij al of niet heimelijk in de gaten gehouden door op zijn harde schijf 'cookies', en andere elektronische spionnen te plaatsen of interactieve middelen ('tools') zoals Reel.com's 'Mood Matcher' of 'Planet Rx's' in te zetten voor psychografische gegevens?

Technology assessment

De Registratiekamer heeft al jarenlang als strategie om pro-actief in te spelen op haar omgeving. Dit geldt ook voor de technologische ontwikkelingen, waarmee zij in toenemende mate wordt geconfronteerd. Binnen het kader van haar wettelijke activiteiten tracht de Registratiekamer vroegtijdig nieuwe en veelbelovende technologieën te analyseren op mogelijk positieve of negatieve effecten voor de (informationele) privacy door middel van technology assessments.

Deze onderzoeken richten zich met name op ICT-technologieën en -toepassingen die de laboratoriumfase hebben verlaten en klaar staan om op de markt geïntroduceerd te worden. Daarbij wordt gekeken naar de aangeboden functionaliteit en de te verwachten effecten op de (informationele) privacy. Voorts richt de analyse zich op push- en pullfactoren en hoe deze nieuwe

toepassingen van wetenschap en technologie zich tot de bestaande privacywetgeving verhouden. Deze onderzoeken hebben een 'early warning' functie. De kennis die hieruit wordt verkregen, is bepalend voor het beleid van de Registratiekamer ten aanzien van de effecten van de onderzochte technologieën.

Beschermen van verkeersgegevens
Het inzetten van MIX nodes in telecom- en andere netwerken lijkt veelbelovend voor het beschermen van de verkeersgegevens van de zender en de ontvanger. Met een serie van mix nodes en een bepaalde toepassing van en- en decryptie kunnen onder andere verkeersgegevens zo worden gemodificeerd en gehergroepeerd dat het vrijwel onmogelijk is om vast te stellen of een bericht "binnenkomt" of "uitgaat". Daarmee kan de analyse van verkeersgegevens worden voorkomen. De resultaten van het onderzoek naar het gebruik van MIX nodes zijn gepresenteerd op een conferentie van het International Computer Science Institute in Berkeley (California).

Een privacyvriendelijke elektronische butler
In de in 1999 gepubliceerde studie *Intelligent software Agents and Privacy* heeft de Registratiekamer gewezen op de gevaren van het teveel aan informatie en de vaak voorkomende opstoppingen op de elektronische snelweg. Dit stimuleert de ontwikkeling van intelligente software agents (ISA) als opvolgers van de zoekmachines. Toepassingen worden vooral gezocht in het inzetten van intelligente software agents als persoonlijke digitale assistenten (elektronische butlers). Een agent zal in de meest vergaande vorm een soort 'alter-ego' worden voor zijn gebruiker. De agent beschikt immers over een schat aan informatie over de persoon die hij vertegenwoordigt. Bij het zoeken en het doen van zaken op internet moeten persoonsgegevens worden uitgewisseld en vergeleken. Hoe kan de gebruiker van een agent er nu op vertrouwen dat zijn gegevens niet ergens terechtkomen waar ze niet horen te komen? Hoe weet je zeker dat de agent alleen de gegevens verstrekt die ter zake zijn of waarvan je zelf goed vindt dat ze worden verstrekt?

Als vervolg op deze studie participeert de Registratiekamer samen met TNO, de Technische Universiteit Delft en acht commerciële bedrijven uit de EU en Canada in het door de EU gesubsidieerd project PISA (privacy incorporated software agent). Daarin zal binnen drie jaar een elektronische butler worden ontwikkeld die zelfstandig de door de internetgebruiker opgedragen taken snel uitvoert en tegelijkertijd de privacy van de gebruiker beschermt. Het internationale PISA consortium zal een privacy threat analysis maken die als basis zal dienen voor de bouwtekeningen (architectuur) van een werkende proefversie van PISA die de privacyrisico's volledig zal ondervangen. De architectuur zal in 2002 beschikbaar zijn. De proefversie zal rond 2004 klaar zijn en kan dan op de website www.pet-pisa.org door iedereen worden getest.

Privacy-Enhancing Technologies
Wanneer organisaties wordt gevraagd welke maatregelen zij hebben getroffen om de privacy te beschermen, dan wijzen zij er steevast op dat zij zich hebben ingespannen om de persoonsgegevens te beveiligen. Hoewel het gebruik van beveiligingsmaatregelen om ongeautoriseerde toegang tot persoonsgegevens te voorkomen een belangrijke component van privacybescherming is, is een dergelijke beveiliging op zich niet toereikend. De gegevens van betrokkenen zijn immers vrijwel nooit versleuteld opgeslagen en de bescherming van de privacy is daarmee totaal afhankelijk van het correct functioneren en uitvoeren van de beveiligingsmaatregelen.

Het verdient daarom de voorkeur technologische maatregelen te nemen waarmee de privacy van het individu direct bij het verzamelen beschermd wordt. Het gaat dan om technologische maatregelen die ervoor zorgen dat er geen enkel gegeven wordt gegenereerd en vastgelegd. Het kunnen echter ook technologische maatregelen zijn die ertoe bijdragen dat het gebruik en de opslag van identificerende gegevens tot een minimum wordt beperkt of zelfs achterwege blijft.

Toepassing van de informatie- en communicatietechnologie (ICT) voor privacybescherming is bekend geworden onder de naam Privacy-Enhancing Technologies (PET). Hierbij worden juridische normen vertaald in technologische specificaties. PET wordt gedefinieerd als: *een samenhangend geheel van ICT maatregelen dat de persoonlijke levenssfeer beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem.*

PET is in artikel 13 van de Wet bescherming persoonsgegevens (WBP) opgenomen en heeft inmiddels een belangrijke plaats in het praktisch en theoretisch repertoire van privacybeschermende middelen ingenomen.

Gezien het wettelijk voorgeschreven basisniveau van privacybescherming zal duidelijk zijn, dat – wil privacy in technologisch opzicht adequaat beschermd worden – er dus meer moet gebeuren dan alleen maar informatiebeveiliging, namelijk het inzetten van PET. Artikel 13 WBP heeft dan ook gevolgen voor de verantwoordelijken voor persoonsgegevens, bewerkers en systeemontwikkelaars.

In augustus 1995 verscheen de publicatie *Privacy-Enhancing Technologies: The Path to Anonymity*, dat in nauwe samenwerking met TNO/FEL te Den Haag en de Information and Privacy Commissioner van de Canadese provincie Ontario te Toronto geschreven was. In het rapport wordt aangetoond, dat het vaak niet nodig is de identiteit van de gebruiker, consument of burger te weten. Er zijn evenwel situaties waar – soms om wettelijke redenen – de identiteit wel bekend moet zijn, bijvoorbeeld bij het betalen voor het gebruik van bepaalde dienstverlening of bij het openen van een bankrekening.

Bij het inzetten van PET om de privacy te beschermen, kan de verantwoordelijke voor verschillende strategieën kiezen:
1. hij richt zich op het voorkomen of verminderen van de identificeerbaarheid;
2. hij zet in, conform de WBP, op het voorkomen van onrechtmatig verwerken van persoonsgegevens;
3. hij gebruikt andere technologieën die de privacy ondersteunen.

Een combinatie van deze strategieën is natuurlijk ook denkbaar. Daarnaast zal de verantwoordelijke vaak ook organisatorische maatregelen nemen.

NBIS en Loket aan Huis.nl

In het kader van het gebruik van internet bij het verwerken van persoonsgegevens heeft de Registratiekamer in 2000 in twee interessante proefprojecten geadviseerd over PET- toepassingen. Het eerste proefproject, het Nederlandse Brandwonden Informatie Systeem (NBIS), staat onder leiding van de Nederlandse Brandwonden Stichting. De architectuur van NBIS zal, bij een met succes afgeronde proef in 2001, de blauwdruk vormen voor het European Burns Information System (EBIS).

Het tweede proefproject betreft een samenwerking tussen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid (met medewerking van diverse organisaties op het terrein van de sociale zekerheid): 'loket aan huis.nl' in Delft.

De proefopstellingen van beide proefprojecten zijn in 2000 voltooid en op basis hiervan zijn begin 2001 actuele tests operationeel waarbij gevoelige persoonsgegevens over internet verstuurd worden. Bij deze projecten is een opeenstapeling van Privacy-Enhancing Technologies gebruikt waarmee voldoende garanties voor een privacyveilige verwerking van persoonsgegevens worden geboden. Het project in Delft maakt namelijk gebruik van biometrie (vingerscan en stem) voor het authenticeren van de gebruikers van de ontwikkelde informatiesystemen. Een Trusted Third Party (TTP) is opgenomen voor het vaststellen van de identiteit op basis van genoemde biometrische kenmerken. Zowel in het Delftse project als bij NBIS wordt encryptie toegepast voor zowel het versleuteld versturen van persoonsgegevens als ook voor de versleutelde opslag van de persoonsgegevens in databases

TTP's, PKI en digitale certificaten

Nederland staat aan de vooravond van grootschalige invoering van TTP's, zowel publiek als privaat. Uit de Wet bescherming persoonsgegevens (WBP) volgt dat wie persoonsgegevens verwerkt, passende technische en organisatorische maatregelen moet nemen om deze gegevens goed te beveiligen. Dat kan door de inzet van TTP's, Public-key infrastructure (PKI) en digitale certificaten. Centraal stond in het onderzoek dat in het verslagjaar werd gedaan, de privacyveiligheid en betrouwbaarheid van communicatie over open netwerken.

Het onderzoek dat in 2001 zal worden gepubliceerd, richt zich op modellen voor 'PET-certificaten'. Deze certificaten beschermen door het gebruik van pseudoniemen de privacy. Het onderzoek concludeert onder meer:

1. Digitale certificaten en verwante cryptografische technieken kunnen een belangrijke rol spelen als Privacy-Enhancing Technology (PET).
2. Anonieme of pseudonieme certificaten hebben waar mogelijk de voorkeur boven identiteitscertificaten. De X.509-standaard beschermt de privacy onvoldoende.
3. Het gebruik van een algemeen persoonsnummer is ongewenst. PKI's dienen zo ingericht te worden dat certificaatnummers of openbare sleutels niet kunnen verworden tot alternatieve persoonsnummers. Nog sterker geldt dit voor biometrische templates.

Cookies killers en anonymizers

De Registratiekamer heeft bijgedragen aan het rapport over internet en privacy van de onder de artikel 29 werkgroep ressorterende Internet Task Force. Hierover is elders in dit jaarverslag gerapporteerd. Relevant is dat in dit rapport gewezen wordt op de technologische mogelijkheden om 'cookies' uit te schakelen en te werken met 'anonymisers' die persoonsgegevens van internetgebruikers anonimiseren voordat die internet opgaan. Eveneens is het mogelijk om filters te gebruiken voor het zeven en weren van e-mail. De Registratiekamer onderschrijft het standpunt van de Internet Task Force met betrekking tot P3P (platform for privacy preferences), waarbij het de bedoeling is dat langs een gestructureerde weg websites hun privacybeleid kenbaar maken aan gebruikers, die vervolgens dan op grond daarvan kunnen besluiten de site wel of niet te bezoeken. P3P is echter niet in staat de privacy van gebruikers te beschermen in landen met een inadequate privacywetgeving. Evenmin kan P3P

ervoor zorgen dat bedrijven zich houden aan hun privacypolicies. De inzet van PISA kan op termijn meer waarborgen verschaffen voor de internetgebruiker.

Publiek debat over biometrische identificatie

In het verslagjaar het de Registratiekamer in samenwerking met het Openbaar Ministerie en de Taakorganisatie Vreemdelingenzorg een publiek debat georganiseerd over biometrische identificatie. Dit naar aanleiding van het rapport dat de Registratiekamer heeft uitgebracht over biometrische identificatie onder de naam *At face value, on biometrical identification and privacy* (Achtergrondstudies en Verkenningen nr. 15, 1999)'. Dit rapport was een verkenningsstudie naar de, te verwachten, grootschalige toepassingen van biometrie. De dienstverlenende kant van biometrische identificatie staat buiten kijf. Biometrische identificatie kan als uitstekend alternatief voor de huidige pincodes en wachtwoorden dienen. Wel is het van belang het verschil te zien tussen één op n identificatie en één op één identificatie. In plaats van identificatie is het beter uit te gaan van verificatie.

In het publieke debat zijn twee doeleinden belicht: opsporing en toegangscontrole. Dit leidt tot de volgende vier randvoorwaarden:

1. voor de betrokkenen moet helder zijn wat er met de opgeslagen biometrische gegevens gebeurt;
2. opslag van biometrische gegevens moet noodzakelijk zijn in relatie tot het doel waarvoor het bestemd is;
3. het minst ingrijpende alternatief voor de persoonlijke levenssfeer dient te worden gekozen;
4. Gezondheids- of rasgegevens mogen in beginsel niet worden opgeslagen, tenzij dat onvermijdelijk is voor een relevant doel en de betrokkene daarmee instemt.

IP adressen

In het verslagjaar heeft de Registratiekamer een onderzoek uitgevoerd naar de vraag of een verwerking van internetadressen in alle gevallen onder de reikwijdte van de Wet persoonsregistraties valt. In het algemeen is vastgesteld dat het zogenaamde IP-adres als persoonsgegeven geclassificeerd moet worden. In dit onderzoek werd een database beoordeeld waarin alle IP-adressen zijn vastgelegd met daarbij de meest waarschijnlijke taal die een gebruiker van een IP-adres spreekt. De eigenaar van een website wordt met behulp van deze database in de gelegenheid gesteld de bezoekers van zijn site direct in de meest waarschijnlijke taal aan te spreken. Het onderzoek heeft, onder voorwaarden, vastgesteld dat in dit geval een verwerking van IP-adressen niet onder de reikwijdte van de privacywetgeving valt.

Discopas

Een aantal eigenaren van discotheken heeft een initiatief ontplooid om de veiligheid van hun bezoekers beter te kunnen garanderen. Hierbij worden bezoekers voorzien van een identiteitspas waaraan een verwerking van persoonsgegevens is verbonden die onrechtmatige of ongewenste toegang moet voorkomen. Voor het onomstotelijk vaststellen van de identiteit van een bezoeker wordt gebruik gemaakt van herkenning op basis van twee biometrische kenmerken: vinger- en gezichtsscan. De Registratiekamer heeft in het verslagjaar het systeem, bij de leverancier, onderzocht tegen de achtergrond van twee van haar Achtergrondstudies en Verkenningen die handelen over de privacyaspecten van een dergelijk informatiesysteem. Deze studies zijn: *At face value* over biometrie en *Belangen en effecten van waarschuwingssystemen* over het gebruik van zwarte lijsten'. Het onderzoek zal begin 2001 worden afgerond.

Handhaving

Als toezichthouder heeft de Registratiekamer een aantal instrumenten tot haar beschikking om naleving van de wettelijke bepalingen te bevorderen. Zij kan de aanmeldingen van persoonsregistraties marginaal toetsen. Bij geschillen over inzage, correctie en verwijdering van persoonsgegevens, kan de Registratiekamer bemiddelen of adviseren. Naar aanleiding van andere klachten – maar ook ambtshalve – kan zij een onderzoek instellen. Bij het uitvoeren van een privacy audit wordt volgens een vaste methodiek onderzocht in hoeverre een persoonsregistratie voldoet aan de wet. De invoering van de Wet bescherming persoonsgegevens (WBP) leidt tot het beschikbaar komen van enkele nieuwe instrumenten, zoals de mogelijkheid tot directe interventie. De Registratiekamer bereidt zich zorgvuldig voor op de invoering van de nieuwe wet.

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 of maatschappelijke dienstverlening moeten voor elke persoonsregistratie een privacyreglement 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 verzameld worden en hoe een organisatie daarmee omgaat. De Registratiekamer toetst de aanmeldingsformulieren marginaal. Bij de behandeling van klachten is het aanmeldingsformulier echter een belangrijk document.

Eind 1999 waren in totaal 63.400 bestanden bij de Registratiekamer aangemeld en in 2000 werden daar 2.577 bestanden aan toegevoegd (zie bijlage 1). De aanmeldingsplicht of de plicht een privacyreglement 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 (WPR) blijft overigens wel van toepassing op registraties die zijn vrijgesteld van de aanmeldingsplicht.

In de loop van 2001 wordt de WPR vervangen door de WBP. Door de invoering van de WBP verandert de systematiek ten opzichte van de WPR. Dit betekent dat alle organisaties zich bij de invoering van de WBP in principe opnieuw moeten aanmelden bij het College bescherming persoonsgegevens (de huidige Registratiekamer) of bij een functionaris voor de gegevensbescherming, voor zover die in de organisatie is aangesteld. Hiervoor geldt volgens de wet een overgangstermijn van een jaar, gerekend vanaf de datum van het inwerkingtreden van de WBP. Nieuwe verwerkingen moeten direct worden aangemeld. Voor de aanmelding zullen nieuwe middelen worden ontwikkeld, zoals een vrijstellings- en meldingsprogramma die op diskette of cd-rom beschikbaar worden gesteld en gedownload kunnen worden van de internetsite van de Registratiekamer. Zij adviseert eenieder om waar mogelijk te wachten tot de middelen voor het doen van een elektronische aanmelding gereed zijn.

Er is geen aanmeldingsplicht als het soort gegevensverwerking genoemd wordt in het Vrijstellingenbesluit (de opvolger van het Besluit Genormeerd Vrijstelling onder de WPR). Zo'n gegevensverwerking moet dan wel voldoen aan de eisen die worden omschreven in het Vrijstellingenbesluit. Hierover zal nog de nodige informatie beschikbaar komen.

Bemiddeling en klachtenbehandeling

Op grond van de WPR en de Wet politieregisters (Wpolr) kan iemand over wie gegevens in een bestand zijn opgenomen, de Registratiekamer verzoeken te bemiddelen of te adviseren wanneer er een conflict is met de verantwoordelijke houder van 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. De Registratiekamer kan ook bemiddelen of adviseren bij een geschil over verbetering of verwijdering van gegevens van de geregistreerde. Daarnaast kan zij op verzoek van een belanghebbende 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 advies of bij een klacht, onderzoekt het frontoffice 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 betrokken organisatie. Ook wordt bezien of er binnen de betreffende sector een klachtenregeling geldt die beter eerst doorlopen kan worden, en of de zaak niet al in behandeling is bij een rechterlijke instantie. 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 meestal de weg naar de rechter open.

Sommige verzoeken kunnen beter door andere instanties behandeld worden, waarbij de Registratiekamer op de achtergrond van advies dient. Dit is bijvoorbeeld het geval wanneer patiënten inzage vragen in een medisch dossier, omdat zij ontevreden zijn met de behandeling. De Registratiekamer kan wel bemiddelen over het inzagerecht, maar kan geen uitspraak doen over de kwaliteit van de behandeling. Door deze beperkte bevoegdheden is zij niet altijd in staat om een conflict geheel op te lossen, terwijl andere instanties (zoals een Informatie- en Klachtenbureau Gezondheidszorg) dat wel kunnen 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.

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 beschikt over bijzondere bevoegdheden voor het doen van een onderzoek naar aanleiding van een klacht: de registratiehouder moet de nodige inlichtingen geven en alle overige medewerking verlenen. Een onderzoek kan leiden tot een openbaar rapport.

In 2000 bemiddelde of adviseerde de Registratiekamer bij 142 conflicten. Vaak ontstonden conflicten doordat geweigerd werd om inzage te verlenen of een kopie van een dossier te verstrekken. Ook lijken sommige direct marketeers zich

weinig aan te trekken van een verzoek om verwijdering van gegevens waardoor mensen nog steeds ongewenste reclame ontvangen.

In totaal werden 181 klachten onderzocht. De meeste klachten gaan over het onterecht verstrekken van persoonsgegevens aan derden. Het komt bijvoorbeeld steeds vaker voor dat vrijetijdsverenigingen hun ledenlijst op internet publiceren of verstrekken aan een geïnteresseerde die graag reclame wil maken bij de leden van de vereniging. Een aantal 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 gegevens die een dergelijk bureau en een telecomaanbieder gebruiken, vandaan komen. Over dit onderwerp is in oktober het rapport *De gewaardeerde klant* verschenen.

Geschil tussen politiefunctionaris en twee inlichtingendiensten

Persoonsgegevens zeggen iets over de wijze waarop een individuele natuurlijke persoon aan het maatschappelijk leven deelneemt. Het gegeven kan bepalend zijn voor de wijze waarop de betrokken persoon in de maatschappij wordt beoordeeld of behandeld. Zo kan belastende informatie over een werknemer vergaande gevolgen hebben voor de arbeidsrelatie met zijn werkgever. Dit probleem is des te groter als de betrokken persoon de betrouwbaarheid en juistheid van deze gegevens niet kan controleren omdat deze gegevens in verband met bronafscherming door een criminele inlichtingendienst geheim worden gehouden. De volgende zaak is daar een treffend voorbeeld van.

De Registratiekamer heeft in het kader van de Wpolr bemiddeld bij twee geschillen tussen een politiefunctionaris (verder: verzoeker) en twee criminele inlichtingendiensten (CID I en CID II). Verzoeker had geconstateerd dat er belastende criminele informatie over zijn vermeende contacten met criminelen in politiekringen circuleerde. Om deze reden werd verzoeker van een groot politieonderzoek afgehaald en werd tegen hem een strafrechtelijk onderzoek ingesteld. De strafzaak eindigt met een sepot wegens het ontbreken van wettig bewijs. De bron van de beschuldigingen werd niet aan verzoeker bekend gemaakt. Omdat hij meer helderheid over de ingebrachte beschuldigingen wil hebben, verzoekt hij twee inlichtingendiensten om inzage in zijn persoonsgegevens.

Verzoeker krijgt te horen dat geen informatie over hem in het register van CID I is vastgelegd. Dit verbaast hem, omdat de minister van Justitie aan de Nationale ombudsman had bevestigd dat informatie over verzoeker was opgeslagen in het CID-register. Ter plaatse constateert de Registratiekamer dat CID I wel mutaties over verzoeker heeft opgeslagen – anders dan de CID noemde – in een CID-register. CID I ging er namelijk vanuit dat het politieregister waarin deze mutaties waren vastgelegd niet als CID-register kon worden aangemerkt. Na bemiddeling van de Registratiekamer heeft CID I haar standpunt gewijzigd en verzoeker alsnog (gedeeltelijke) inzage gegeven.

CID II had verzoeker bericht dat zij geen persoonsgegevens over hem in haar registers had opgeslagen. De minister van Justitie had echter aan de Nationale ombudsman laten weten dat CID II de werkgever van verzoeker had geïnformeerd over een omgekochte politiefunctionaris bij een criminele organisatie. In het kader van de bemiddeling is echter aannemelijk geworden dat CID II geen persoonsgegevens over verzoeker heeft vastgelegd. De bij deze CID vastgelegde criminele informatie had namelijk betrekking op een andere

persoon en zijn werkgever heeft deze gegevens dus ten onrechte aan verzoeker toegeschreven.

Onderzoek ambtshalve

De Registratiekamer kan ook besluiten om uit eigen beweging een onderzoek in te stellen. In de praktijk gebeurt dat diverse keren per jaar. Het kan daarbij gaan om bepaalde incidenten, maar ook om ervaringen over mogelijke misstanden die bij de behandeling van andere zaken zijn opgedaan. Aan het besluit om een onderzoek in te stellen gaat vaak een informatieve ronde vooraf. Indien uit een dergelijke eerste ronde blijkt hoe de zaak er voor staat (er is bijvoorbeeld sprake van onwetendheid of een vergissing die direct kan worden rechtgezet), dan is er doorgaans onvoldoende reden om tot een diepergaand onderzoek te besluiten.

In het rapport *De gewaardeerde klant; privacyregels voor credit scoring* zijn aanbevelingen gedaan die een leidraad vormen voor een zorgvuldige en rechtmatige verwerking van persoonsgegevens in de (handelsinformatie) praktijk. Uit diverse bronnen vernam de Registratiekamer dat een handelsinformatiebureau op indringende wijze bepaalde instanties benaderde met het verzoek om informatie over personen. Diverse instanties waarvoor een geheimhoudingsverplichting geldt, informeerden de Registratiekamer hier geregeld over. Zij heeft in het licht hiervan besloten om een onderzoek ter plaatse te verrichten. De Registratiekamer heeft daarbij gebruik gemaakt van de bevoegdheden verleend in de WPR en de Algemene wet bestuursrecht.

Vóór, tijdens en na het onderzoek ter plaatse is medewerking verkregen van het Nederlands Forensisch Instituut (NFI), de Nederlandse Mededingingsautoriteit (NMa) en het Interregionaal Team Digitale Experts (ITDE) van de politie Haaglanden. Ter plaatse is bij het informatiekantoor bewijsmateriaal verkregen (digitaal en papier) en vervolgens op diverse locaties geanalyseerd. Het NFI, de NMa en het ITDE hebben de onderzoekers van de Registratiekamer geadviseerd over de operationele aspecten van een onderzoek. Het NFI en het ITDE hebben zeer effectief en efficiënt medewerking verleend tijdens de analyse van het digitale materiaal. De analyse van bevindingen is vastgelegd in een rapportage. Dit rapport van bevindingen is voorgelegd aan het betreffende informatiebureau. Het uiteindelijke rapport is – met inachtneming van het principe van hoor en wederhoor – in het eerste kwartaal van 2001 vastgesteld.

Audits

In het kader van de voorbereiding van het rapport *Klant in het Web* zijn fact-finding onderzoeken uitgevoerd bij een aantal Internet Service Providers. Een fact-finding onderzoek bestaat uit een IT-audit waarbij de auditor van de Registratiekamer vaststelt welke persoonsgegevens en voor welk doel in de computersystemen van de onderzochte partij worden verwerkt. Deze onderzoeken zijn uitgevoerd bij een aantal representatieve aanbieders van internetdiensten, waaronder zowel betaalde als gratis providers. De onderzoeken hadden voornamelijk betrekking op twee aspecten van de werkzaamheden bij de provider: welke persoonsgegevens worden er verzameld en verder verwerkt in het kader van de relatie tussen abonnee en provider (accountgegevens), en welke persoonsgegevens ontstaan doordat de abonnee internetdiensten afneemt (verkeersgegevens). Het onderzoek had tot doel vast te stellen in welke situaties er sprake is van een contract, welke gegevens de provider nodig heeft voor het kunnen leveren van internetdiensten en welke bewaartermijn gehanteerd wordt voor deze gegevens. Daarnaast werd geïnventariseerd welke extra persoonsgegevens er werden verzameld en de daarvoor gebruikte bewaartermijn. De resultaten van het onderzoek zijn in het rapport verwerkt.

Nationaal Schengen Informatie Systeem

In 1997 heeft de Registratiekamer een privacy-audit uitgevoerd naar de kwaliteit van de bescherming van de gegevens over personen die in de politieregisters van het Nationaal Schengen Informatie Systeem (NSIS) zijn geregistreerd. De audit resulteerde is een aantal aanbevelingen ter verbetering van het NSIS. Na implementatie van deze aanbevelingen zou het NSIS beter voldoen aan de geldende privacywetgeving.

In 2000 is een controle audit uitgevoerd om vast te stellen op welke wijze de betrokken organisaties gehoor hadden gegeven aan de aanbevelingen. Deze controle audit werd uitgevoerd op een drietal locaties: de IT-Organisatie in Driebergen, het bureau Sirene in Zoetermeer en de Politie Midden- en West-Brabant. De controle activiteiten hebben zich geconcentreerd op de aanbevelingen die de Registratiekamer bij de uitgevoerde privacy audit heeft gedaan ter verbetering van de bescherming van de persoonlijke levenssfeer. Over het algemeen heeft de Registratiekamer vastgesteld dat de drie organisaties voortvarend actie hebben ondernomen op de gedane aanbevelingen. Op enkele gebieden was de voortgang onvoldoende. Op deze gebieden zal de Registratiekamer in 2001 een nadere controle audit uitvoeren.

Proefproject criminele inlichtingen

Op verzoek van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft de Registratiekamer geparticipeerd in een juridische audit bij de Criminele Inlichtingen Eenheid (CIE) van een regionaal politiekorps.

Het onderzoeksteam bestond uit een privacyfunctionaris van een ander politiekorps, een officier van justitie en een juridisch beleidsmedewerker van de Registratiekamer. Een externe deskundige uit het bedrijfsleven coördineerde het geheel. Het onderzoek is beperkt tot de inhoud van de registers van de CIE: het informantenregister, het voorlopig register en het register zware criminaliteit. Uitgangspunt daarbij was de werking van de bescherming van de persoonlijke levenssfeer.

De feitelijke werking van deze registers is in dat kader vergeleken met de juridische normen die de wetgeving voor (bijzondere) politieregisters stelt. Primair object van onderzoek waren de noodzaak en de rechtmatige verkrijging van de vastgelegde criminele inlichtingen en informantgegevens. In dat kader zijn de registers van de CIE – aan de hand van een aantal natuurlijke personen en rechtspersonen mét hun relaties die object van onderzoek zijn voor de CIE – doorgelicht op de kwaliteitscriteria juistheid, rechtmatigheid, volledigheid, tijdigheid en toereikendheid.

Voorafgaand aan de inhoudelijke beoordeling van de zaken werden enkele medewerkers van de CIE en het Openbaar Ministerie op sleutelposities geënquêteerd. Een tevoren opgestelde vragenlijst en checklist met toetsingscriteria vormden daarbij het uitgangspunt. Voornaamste aspecten van beoordeling waren het ‘wegzetten’ van de criminele informatie, de controle van en het toezicht op de betrouwbaarheid, actualiteit, volledigheid en rechtmatigheid van de opgenomen gegevens, alsmede de wijze waarop vastgelegde gegevens intern en extern worden verstrekt.

De opgedane ervaringen zullen onder meer ten grondslag liggen aan een door het ministerie van BZK te ontwikkelen en verplicht te stellen auditaanpak binnen alle CIE-en van de politie.

Ontwikkeling Auditaanpak

Eind 1999 heeft de Registratiekamer het initiatief genomen voor de ontwikkeling van een auditaanpak voor privacy audits. In samenwerking met marktpartijen, zoals audit- en adviesorganisaties, koepelorganisaties van auditors, werknemers-, werkgevers- en consumentenorganisaties en de ministeries van Justitie en BZK is in 2000 voortvarend gewerkt aan de realisering van drie auditproducten: Quickscan, WBP Zelfevaluatie (eventueel met review) en Raamwerk Privacy Audit. Dit initiatief past binnen de beleidsfilosofie van de Registratiekamer tot het stimuleren van zelfregulering. De auditproducten zijn eind 2000 vastgesteld en zijn in het eerste kwartaal van 2001 voor eenieder beschikbaar gesteld via de website van de Registratiekamer www.registratiekamer.nl.

De auditproducten zijn generiek van opzet, zodat ze door alle typen van organisaties gebruikt kunnen worden, en richten zich uitsluitend op de WBP. Door verschillende instanties zijn reeds initiatieven genomen om te komen tot sectorspecifieke auditproducten, gebaseerd op de generieke auditproducten. De auditproducten stellen organisaties in staat om de kwaliteit van de getroffen maatregelen voor de bescherming van persoonsgegevens in een organisatie te beoordelen en te toetsen. Tussen de verschillende auditproducten bestaat een niveauverschil, zodat een goede afweging gemaakt moet worden bij de keuze van de auditproducten.

De Quickscan is een beknopte vragenlijst waarmee functionarissen binnen een organisatie snel inzicht kunnen verkrijgen in de mate waarin men zich bewust is van de bescherming van persoonsgegevens. De vragen zijn geclusterd in vier categorieën: privacybewustzijn in de organisatie, uitvoering wettelijke bepalingen, beveiliging en controle. De uitkomsten geven een globale indruk hoe het met de privacybescherming in een organisatie gesteld is.

De Quickscan is met name geschikt voor het creëren van bewustwording en kan het begin zijn van een verbetertraject in de organisatie. De Quickscan bevat een duidelijke toelichting op het gebruik en kan door alle werknemers in een organisatie ingevuld worden. De uitkomsten zijn nuttig voor de leiding, de ondernemingsraad en, indien benoemd, voor de functionaris voor de gegevensbescherming. Op de website van de Registratiekamer is een uitgebreide toelichting op de verschillende mogelijke antwoorden beschikbaar. Aan de hand van deze toelichting kunnen de mogelijke vervolgstappen bepaald worden.

Via de WBP Zelfevaluatie kan een organisatie zelfstandig en in betrekkelijk korte tijd de kwaliteit van de maatregelen voor de bescherming en beveiliging van persoonsgegevens beoordelen. De methode is gebaseerd op het INK-model, dat beoogt de leiding van een organisatie zelf te laten vaststellen hoe de organisatie presteert en hoe de organisatie is ingericht op haar taak. De organisatie kan via de WBP Zelfevaluatie zowel haar ambitieniveau voor de bescherming van persoonsgegevens aangeven, als de feitelijke beoordeling. Daarbij zijn de bepalingen van de WBP overzichtelijk geclusterd in negen aandachtsgebieden die alle aspecten van de WBP afdekken. Per aandachtsgebied worden ook de sterke punten en de punten voor verbetering geïdentificeerd. Tot slot worden alle bevindingen samengevat, waarbij in één oogopslag duidelijk is hoe de feitelijke naleving van de bescherming van persoonsgegevens zich verhoudt ten opzichte van het gedefinieerde ambitieniveau. Organisaties kunnen de WBP Zelfevaluatie ook gebruiken bij de implementatie van de WBP binnen de organisatie of de overgang van WPR naar

WBP. De WBP Zelfevaluatie bevat een praktische handreiking bij de voorbereiding en uitvoering van het instrument.

De WBP Zelfevaluatie kan desgewenst met een review worden uitgebreid. De review, door een in- of externe deskundige, verhoogt de waarde van de interne meting. De leiding krijgt zo een uitkomst voorgelegd die is gebaseerd op een onafhankelijke toetsing van daadwerkelijk getroffen maatregelen in de organisatie.

Het Raamwerk Privacy Audit is bedoeld voor het uitvoeren van een privacy audit door een deskundige interne of externe auditor. De rapportering van de privacy audit geeft de leiding van een organisatie met een hoge mate van zekerheid een objectief beeld van de naleving van de wettelijke bepalingen en daarmee ook inzicht in de sterke en zwakke punten van de bescherming van persoonsgegevens. De Registratiekamer is met beroepsorganisaties van auditors in overleg over een applicatiecursus voor accountants en IT-auditors die privacy audits willen uitvoeren.

De auditproducten zijn tijdens de ontwikkeling uitgebreid getest bij verschillende typen van organisaties. De ervaringen en bevindingen bij het gebruik van de auditproducten zullen gebruikt worden voor verdere optimalisering van de nu ontwikkelde producten.

In aansluiting op de auditproducten is een project gestart om de haalbaarheid van een privacycertificaat te onderzoeken. Een privacycertificaat kan als keurmerk een belangrijke rol vervullen bij zelfregulering door organisaties. De Registratiekamer stelt daarbij als eis dat een toekomstig privacycertificaat voldoet aan hoge kwaliteitseisen. Naar verwachting zal er eind 2001 meer duidelijkheid bestaan over de haalbaarheid van een privacycertificaat.

Overzicht diepgang productenset

Behoefte/diepgang	Product
Globale indruk	Quickscan
Interne meting	WBP Zelfevaluatie
Interne meting + Externe beoordeling	WBP Zelfevaluatie + review
Onafhankelijk onderzoek + certificaat	Privacy Audit

Voorbereiding inwerkingtreding WBP

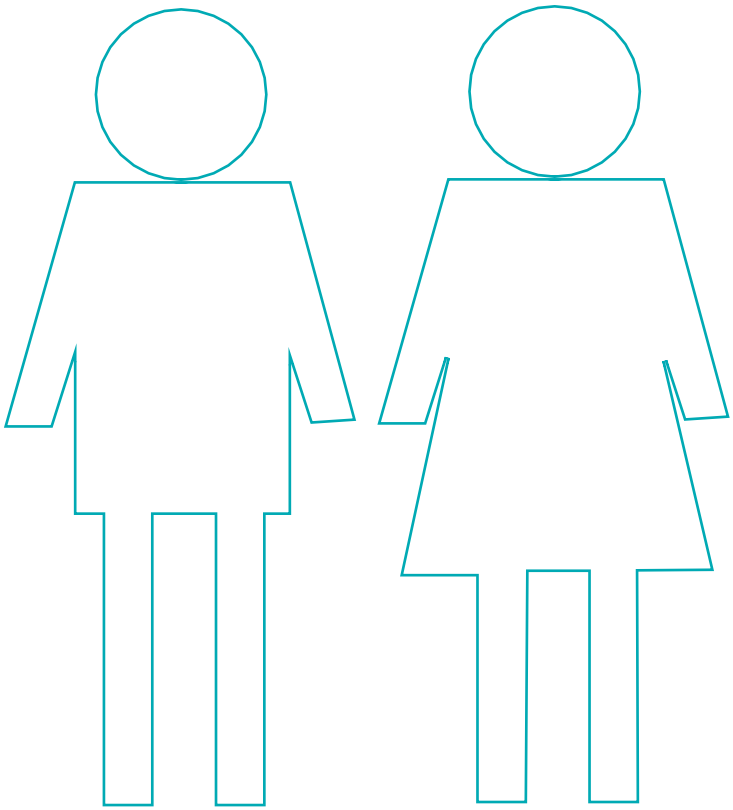
De invoering van de WBP zal leiden tot het beschikbaar komen van nieuwe bevoegdheden, waaronder de mogelijkheid tot directe interventie. Zo zal het CBP de bevoegdheid krijgen om een bestuurlijke boete op te leggen bij niet-aanmelding en een last onder dwangsom op te leggen of bestuursdwang toe te passen bij andere overtredingen. De WBP geeft op deze wijze invulling aan de Europese richtlijn die voorschrijft dat de toezichthouder in staat moet zijn effectief in te grijpen bij overtredingen. Daarmee is sprake van een uitbreiding van de bevoegdheden en zullen aanvullend beleid, nieuwe instrumenten en een nieuwe uitvoeringspraktijk ontstaan. Vooruitlopend op de inwerkingtreding van de WBP heeft de Registratiekamer in 2000 de primaire uitgangspunten voor dit nieuw te ontwikkelen beleid verkend.

Onder het regime van de Wet persoonsregistraties was de Algemene wet bestuursrecht slechts in beperkte mate van toepassing. De uitoefening van de nieuwe bevoegdheden wordt echter mede genormeerd door de in die laatste wet

opgenomen beginselen van behoorlijk bestuur. Deze beginselen zien met name op de voorbereiding, de motivering en de inhoud van de besluiten tot interventie. Bij de bevoegdheid tot het opleggen van een bestuurlijke boete dient bovendien te worden voldaan aan de eisen van 'due process' in artikel 6 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

Deze eisen zullen vertaald worden naar werkprocessen die aan de verscherpte kwaliteitseisen kunnen voldoen. Daarbij gaat het onder meer om functiescheiding bij de behandeling van zaken die aanleiding kunnen geven tot het gebruik van interventiebevoegdheden. Eveneens zal functiescheiding moeten worden toegepast bij de eventueel daarop volgende bezwaar- en beroepsprocedures. In 2000 is hiertoe een aanzet gegeven in de vorm van een inventarisatie van de wettelijke vereisten die gaan gelden bij de inwerkingtreding van de WBP. Voorts zijn de contouren van de organisatorische inbedding van de uitgebreide handhavingstaak neergezet. Ten aanzien van de werkprocessen is een globale verkenning en eerste opzet tot stand gebracht. In de loop van 2001 zal een en ander nader uitgewerkt en gerealiseerd worden. Bij de interne opleidingen is hieraan reeds de nodige aandacht besteed.

Organisatie



De Eerste Kamer heeft op 3 juli 2000 de Wet bescherming persoonsgegevens (WBP) aanvaard. De WBP is de Nederlandse uitwerking van de Europese richtlijn 95/46 EG waarin op Europees niveau vorm wordt gegeven aan privacybescherming. De WBP brengt voor het College bescherming persoonsgegevens (CBP), de opvolger van de Registratiekamer, nieuwe taken en verantwoordelijkheden met zich mee. Deze uitbreiding van wettelijke taken liggen op het gebied van toezicht op en de handhaving van de privacybescherming. Daarnaast is er, meer dan onder de Wet persoonsregistraties, sprake van een internationale dimensie. De WBP regelt nadrukkelijk het samenwerken met Europese zusterorganisaties bij het doen van onderzoeken naar de toepassing van privacyregels.

In Algemene Maatregelen van Bestuur wordt de aanmeldingsverplichting nader geconcretiseerd. Het Vrijstellings- en Meldingsbesluit zijn in het verslagjaar in concept uitgewerkt. Zowel de aanvaarding van de WBP door de Eerste en Tweede Kamer als de toenemende maatschappelijke en politieke belangstelling voor privacyaspecten hebben geleid tot een stijging van het aantal verzoeken om informatie en bemiddeling, het indienen van klachten en het aantal telefonische vragen (zie bijlage 13).

Voorbereiden op de invoering van de WBP

De Registratiekamer is doorgegaan met het voorbereiden van het inwerkingtreden van de WBP. De wetswijziging en de daaruit voortvloeiende consequenties voor bedrijfsleven, overheden en burgers moeten de privacy van iedereen in de samenleving versterken. Deze algemene doelstelling kan geoperationaliseerd worden in twee belangrijke subdoelstellingen die de Registratiekamer zich stelt:

1. Voor overheden, bedrijfsleven en burgers moet de Registratiekamer een toegankelijke organisatie zijn, waar men advies, voorlichting en informatie kan inwinnen op een wijze die past bij de doelgroep. De Registratiekamer is (inter)actief in haar communicatie naar vertegenwoordigers van doelgroepen en stelt daarnaast voorlichtingsmateriaal beschikbaar in de vorm van brochures die ook te raadplegen zijn op de internetsite. De wijze waarop de verschillende doelgroepen op de meest effectieve wijze kunnen worden bediend, behoeft voortdurend aandacht en verdient – zeker met de inwerkingtreding van de WBP – extra aandacht en zorg.
2. Daarnaast moet de meldingsprocedure onder de WBP zodanig zijn ingericht dat zowel grote als kleine organisaties, met zo min mogelijk inspanning aan hun aanmeldingsverplichting kunnen voldoen. Een adequate en efficiënte verwerking van aanmeldingen verkleint de administratieve lasten, sponsort mede daardoor de bereidheid om wettelijke verplichtingen na te leven, maakt de verwerking van persoonsgegevens transparanter en levert zo een belangrijke bijdrage aan het privacybewust omgaan met persoonsgegevens.

Personeelsbeleid

De integriteit is één van de competenties waarin in het afgelopen verslagjaar met nadruk aandacht is besteed. De Registratiekamer en straks het CBP willen immers gezien worden als een betrouwbare partner en toezichthouder die onafhankelijk, zorgvuldig, transparant en controleerbaar optreedt. Voorbeeldgedrag van alle medewerkers is daarvoor een essentiële voorwaarde.

Het ziekteverzuim binnen de Registratiekamer is ten opzichte van 1999 iets teruggedrongen (1999: 8,73%; 2000: 8,15%), maar blijft ook in 2001 een extra zorg waarvoor in samenwerking met de Arbo-dienst maatregelen worden getroffen.

Voor wat de instroom en uitstroom van personeel betreft (zie bijlage 11)

profiteert de Registratiekamer van een verbeterd imago en de toenemende maatschappelijke en politieke belangstelling voor privacybescherming. Gewaardeerde medewerkers hebben hun loopbaan kunnen voortzetten bij organisaties en bedrijven waarin zij hun kennis op het gebied van de privacybescherming in kunnen zetten. De Registratiekamer ervaart dit als één van de positieve effecten waarin zij als tweede-lijnsorganisatie haar doelstellingen bereikt. Bij de instroom van nieuwe medewerkers kan de Registratiekamer – ondanks de druk op de arbeidsmarkt – een goede keuze maken uit het aanbod van gekwalificeerd personeel.

Uiteraard zal de balans van de instroom en uitstroom in evenwicht moeten blijven om te voorkomen dat kennis binnen de organisatie verloren gaat. De inrichting van het kenniscentrum, het beheer van het workflow managementsysteem als kennissysteem, het onderhouden van de standaards en beschrijving van de werkprocessen zijn daarvoor de waarborgen.

Ondernemingsraad

Begin 2000 zijn voor de besturing en de werkwijze van de Registratiekamer twee belangrijke mijlpalen gezet. De interne besturing van de Registratiekamer en het personeelsbeleid is na overleg met de ondernemingsraad vastgesteld. Zij geven een goede basis voor de afspraken en condities waaronder de mensen van de Registratiekamer hun werkzaamheden verrichten. Een vervolg daarop is de aanpassing van het formatieplan van de Registratiekamer. De uitbreiding van de formatie, de formele inbedding van het frontoffice, de inbedding van de nieuwe taken onder de WBP, de ontwikkeling van een kenniscentrum en de invoering van competentiemanagement worden verder uitgewerkt in het formatieplan.

De secundaire arbeidsvoorwaarden zijn in overleg met de ondernemingsraad verbeterd met de ontwikkeling van het vervoersplan. Met het vervoersplan komen de kosten voor openbaar vervoer (2e klas) of de kosten voor de aanschaf van een fiets voor rekening van de Registratiekamer. Op 1 januari 2001 is het vervoersplan ingevoerd.

Het afgelopen jaar heeft de ondernemingsraad met name aandacht gevraagd voor het personeelsbeleid (inclusief opleidingen), het arbo-beleid en de overige secundaire faciliteiten voor medewerkers zoals het vervoersplan. Verder is met de ondernemingsraad de aanpak en inzet voor het formatieplan besproken. De ondernemingsraad levert daarbij op constructieve wijze hun inbreng aan de kwaliteitsverbetering van de organisatie en draagt bij aan de kwaliteitszorg voor het personeel.

Vooruitblik

In dit hoofdstuk wil de Registratiekamer stilstaan bij de belangrijkste activiteiten van het lopende jaar. Het past in het streven naar meer resultaatgerichtheid om daarbij ook op hoofdpunten aan te geven op welke concrete doelen die activiteiten zijn gericht. In het jaarverslag over 2001 zal aan de hand van dit overzicht worden nagegaan in hoeverre deze doelen zijn gehaald.

Dit jaar staat in het teken van de invoering van de Wet bescherming persoonsgegevens. Dat betekent onder meer een overgang van de Registratiekamer naar het College bescherming persoonsgegevens en de invulling van nieuwe taken en bevoegdheden. De Registratiekamer zal zich grondig op deze overgang voorbereiden. Daarnaast zal zij een flinke bijdrage leveren aan een soepele invoering van de wet in de verschillende sectoren van de samenleving.

Het is de bedoeling een ontwikkeling te bevorderen waarbij degenen die verantwoordelijk zijn voor het verwerken van persoonsgegevens, de bescherming van de persoonlijke levenssfeer steeds meer als een vanzelfsprekendheid gaan ervaren en dit inzicht weten te vertalen in hun werkzaamheden. Dit leidt ertoe dat dit jaar sterk de nadruk zal worden gelegd op voorlichting, bewustwording en normontwikkeling.

Het stimuleren van de eigen verantwoordelijkheid van overheden, instellingen en bedrijven neemt een belangrijke plaats in. Het ligt niet voor de hand om in het jaar van de implementatie van de nieuwe wet in te zetten op de handhaving. Wel zullen de voorwaarden worden geschapen om een effectief gebruik van de handhavingsbevoegdheden mogelijk te maken, indien en zodra daartoe aanleiding bestaat.

Naast de activiteiten die rechtstreeks samenhangen met de invoering van de Wet bescherming persoonsgegevens, zullen de gewone werkzaamheden zo goed mogelijk voortgang blijven vinden. Ook hier staat een soepele overgang van WPR naar WBP voorop, waarbij de huidige wet als gevolg van het overgangsrecht nog enige tijd van toepassing zal blijven. Wel zullen hierbij in toenemende mate prioriteiten moeten worden gesteld. In dat verband zijn enkele hoofdonderwerpen van aandacht geselecteerd die richting zullen geven aan de te maken keuzen.

Zo zal de Registratiekamer bijzondere aandacht geven aan de ontwikkelingen op het terrein van de ‘elektronische overheid’, de toepassing van ICT in de gezondheidszorg, de nieuwe vragen op het terrein van e-commerce, sociale zekerheid en reïntegratie, telecommunicatie en verkeersgegevens, en verwerking van criminele inlichtingen bij de politie. Als breder thema staat ook de identificatie van personen in de aandacht. In de meeste gevallen gaat het om meerjarige onderzoeksthema’s waarop in volgende jaarverslagen zal worden teruggekomen.

In 2001 zal met name worden gemikt op de volgende resultaten:

- **Voorlichtingscampagne**
  Rond de invoering van de Wet bescherming persoonsgegevens zal in samenwerking met de ministeries van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties een voorlichtingscampagne worden gehouden. De Registratiekamer verzorgt daarbij met name de voorlichting aan koepel- en brancheorganisaties, en via deze organisaties aan hun leden. Hierbij zal zoveel mogelijk worden ingespeeld op de behoeften van elke branche.

- **Internetsite & informatiemateriaal**
  De internetsite van de Registratiekamer zal opnieuw worden ingericht aan de hand van een sectorsgewijze indeling en een nieuw adres krijgen (www.cbpweb.nl). Deze website zal een centrale plaats krijgen in de communicatiestrategie, waarbij de eigen behoefte van de informatiezoekende burger voorop staat. Alle publicaties zullen op de website gratis beschikbaar zijn. Het bestaande informatiemateriaal zal met het oog op de invoering van de nieuwe wet integraal worden herzien en worden uitgebreid.

- **Zelfregulering**
  Een speciale brochure zal worden uitgebracht over de mogelijkheid om een 'functionaris voor de gegevensbescherming' aan te stellen (artikel 62 e.v. WBP). De werkzaamheden van een functionaris zullen hierin zo concreet mogelijk worden toegelicht. Voorts zal een handleiding worden ontwikkeld voor organisaties die overwegen om een gedragscode te gaan opstellen (artikel 25 WBP).

- **Beveiliging & PET**
  De verplichting om passende maatregelen te treffen ter beveiliging van persoonsgegevens (artikel 13 WBP) zal worden belicht in het rapport Beveiliging van persoonsgegevens. Dit rapport is bedoeld als handreiking aan de praktijk om nadere invulling te geven aan de beveiligingsplicht. In een aparte brochure zal worden ingegaan op de mogelijke inzet van 'Privacy-Enhancing Technologies' (PET).

- **Auditaanpak**
  In een samenwerkingsverband met koepelorganisaties en marktpartijen is een methode ontwikkeld om de kwaliteit van gegevensbescherming binnen organisaties systematisch te beoordelen. De producten van dit gemeenschappelijke project (Quickscan, WBP Zelfevaluatie en Raamwerk Privacy Audit) worden breed toegankelijk gemaakt. In aansluiting daarop zal worden onderzocht of het mogelijk is een certificaat te ontwikkelen voor organisaties die zich met goed gevolg aan een privacy audit hebben onderworpen.

- **Aanmeldingen**
  Met het oog op de invoering van de Wet bescherming persoonsgegevens zal een nieuw systeem worden opgezet voor het aanmelden van verwerkingen bij de toezichthouder. De verwerkers van persoonsgegevens zullen gebruik kunnen maken van een programma om na te gaan of er sprake is van een vrijstelling, en indien nodig de aanmelding te doen. Een en ander zal vergezeld gaan van alle nodige informatie. Aanmelding zal mogelijk zijn op formulier of diskette en uiteindelijk ook geheel via internet.

- **Handhaving**
  Bij de invoering van de nieuwe wet zullen alle voorbereidingen getroffen zijn om effectief gebruik te kunnen maken van de bevoegdheid tot het opleggen van bestuurlijke boete of last onder dwangsom, dan wel het toepassen van bestuursdwang. De uitgangspunten voor het gebruik van deze bevoegdheden zullen worden gepubliceerd.

- **Werkprocessen**
  De werkwijzen en procedures voor de uitoefening van alle overige taken en bevoegdheden zullen nauwkeurig worden beschreven om een goede functiescheiding te waarborgen. De inhoud zal worden verwerkt in informatiemateriaal dat voor iedereen toegankelijk zal zijn.

- **Derde landen**
  Een brochure zal worden ontwikkeld voor instellingen en bedrijven die gegevensverkeer onderhouden met landen buiten de Europese Unie. In deze brochure en daarbij behorende informatie zal worden ingegaan op de mogelijkheden voor dit gegevensverkeer onder de nieuwe wet en de procedure voor het verkrijgen van een vergunning (artikel 77 WBP).

- **Bestuur en organisatie**
  Een bestuursreglement zal worden vastgesteld en ter goedkeuring worden voorgelegd aan de minister van Justitie. De organisatorische consequenties van de overgang naar het CBP zullen worden uitgewerkt in een nieuw formatieplan. Dit zal aanknopingspunten bevatten voor verbetering van het personeelsbeleid en professionalisering van de bedrijfsvoering.

bijlagen

Aanmeldingen

Bijlage 1

Persoonsregistraties aangemeld bij de Registratiekamer van 1 januari 2000 tot en met 31 december 2000, gespecificeerd naar sector.

Arbeid	94
Financiën	126
Handel en dienstverlening	482
ICT en telecommunicatie	12
Marketing	275
Onderwijs en wetenschappen	39
Overheid	88
Politie en justitie	29
Sociale zekerheid	5
Verkeer en vervoer	11
Vrije tijd	80
Zorg en welzijn	1.336
Totaal in 2000	2.577
Totaal aantal geregistreerde aanmeldingen	65.977

Een gedetailleerdere lijst is beschikbaar op de internetsite van de Registratiekamer.

Adviezen over wetsvoorstellen en besluiten

Bijlage 2

Alle adviezen kunt u raadplegen op de website: **www.registratiekamer.nl.** Daarin zijn adviezen opgenomen vanaf 1996. (Adviezen vanaf 1991 zijn ook opgenomen in de bundel *Persoonsgegevens beschermd, Van WPR naar WBP*. Den Haag, Sdu uitgevers, 1999)

Wijziging van de regeling van het DNA onderzoek in strafzaken in verband met het vaststellen van uiterlijke persoonskenmerken aan de hand van celmateriaal
22 december 2000

Wijziging Wetboek van Strafvordering in verband met het verstrekken van strafrechtelijke persoonsgegevens aan derde door het Openbaar Ministerie
12 december 2000

Wetsvoorstel invoering Wet Structuur Uitvoering Werk en Inkomen (SUWI)
28 november 2000

Uitvoeringsbesluit Wet Inkomstenbelasting 2001
17 november 2000

Aanpassing Besluit GBA en aanpassing model verhuisbericht
25 september 2000

Concept wetsvoorstel Structuur Uitvoering Werk en Inkomen (SUWI)
22 september 2000

Wetsvoorstel ter implementatie van de Europese richtlijnen in het kader van elektronische handtekeningen
28 augustus 2000

Wijziging Besluit gebruik sofi-nummer en Besluit politieregisters
25 augustus 2000

Criminele inlichtingen eenheden (CIE-regeling)
15 augustus 2000

Aanpassing van de Regeling Gemeentelijke Basisadministratie persoonsgegevens (GBA) en de Regeling periodieke audit GBA
1 augustus 2000

Wijziging kentekenreglement met betrekking tot de katvangerproblematiek
24 juli 2000

Wetsvoorstel cameraobservatie
17 juli 2000

Invoering persoonsgebonden nummer in het onderwijs
21 juni 2000

Concept Vrijstellingsbesluit (Wet bescherming persoonsgegevens)
7 juni 2000

Concept Meldingsbesluit (Wet bescherming persoonsgegevens)
7 juni 2000

Wet op de jeugdhulpverlening in verband met Advies en Meldpunt Kindermishandeling (AMK's)
16 mei 2000

Wijziging van de Gemeentewet in verband met identificatieplicht voor prostituees
11 mei 2000

Screeningsbevoegdheden van het college van B&W op het gebied van drank- en horecawet
26 april 2000

Besluit bijzondere vergaring nummer-gegevens telecommunicatie, IMSI catcher
31 maart 2000

Huursubsidiewet 2000-2001
20 maart 2000

Cybercrime-verdrag Raad van Europa
13 maart 2000

Besluit DNA-onderzoek in strafzaken
17 februari 2000

Uitvoeringsbesluiten Wet bescherming persoonsgegevens
14 februari 2000

Rapporten

Bijlage 3

Rapporten kunt u doorgaans raadplegen op de website:
www.registratiekamer.nl.

Zorg voor gegevens bij indicatiestelling
Augustus 2000

Politiegegevens beschermd – Een toelichting op het gesloten verstrekkingenregime van de Wet politieregisters
Juni 2000

Het verstrekken van gegevens door de Belastingdienst aan CAK BZ
27 april 2000

Screening van politiepersoneel moet volgens de regels
9 februari 2000

Controle e-mailverkeer door werkgever
27 december 1999

Is Landelijk Alcohol en Drugs Informatiesysteem een persoonsregistratie?
19 november 1999

Onderzoek naar handelsinformatiebureau Goderie van Groen
November 1999

Uitbesteding taken Algemene Bijstandswet
8 september 1999

Werken met gegevens – gegevensuitwisseling tussen CWI's en uitzendbureaus
Augustus 1999

Bijstandsdossiers en bescherming persoonsgegevens
10 juli 1999

Vastleggen en verstrekken van call detail records
24 juni 1999

Verzekeringsmaatschappij verplicht Arbo-dienst tot registratie en rapportage gegevens
14 juni 1999

Verstrekken van gegevens door deurwaarders
30 juni 1999

Handhavingsteams en persoonsgegevens
April 1999

Dealer mag zonder toestemming alleen gegevens aan een auto-importeur verstrekken voor service-ondersteuning
15 februari 1999

Privacy Audit Gemeentelijke Basisadministratie gemeenten Almelo, Breda en Langedijk
5 februari 1999

Privacy Audit Nationaal Schengen Informatiesysteem
December 1998

Doorzenden voorlichtingsrapport reclassering na toestemming
21 december 1998

Medicatiebewaking door centrale patiëntenregistratie
27 oktober 1998

Beroepscode psychologen
14 juli 1998

Reglementering en beveiliging persoonsregistraties door ministeries
9 juli 1998

Gegevens over honden en het verstrekken daarvan
8 juli 1998

Gegevens uit controle door de rijksverkeersinspectie
23 juni 1998

Persoonsgebonden clubcard II
28 mei 1998

Persoonsgebonden clubcard
11 februari 1998

Meldpunt Ongebruikelijke Transacties
Juli 1997

Videocamera's Wallen Amsterdam
21 mei 1997

In beeld gebracht – privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging
27 januari 1997

Als de telefoon wordt opgenomen – regels voor het registreren, meeluisteren en opnemen van telefoongesprekken van werknemers
November 1996

Privacy Audit Handelsinformatiebureau
Juli 1996

Achtergrondstudies en Verkenningen

Bijlage 4

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

Achtergrondstudies en Verkenningen

Terstegge, J.H.J., **Goed werken in netwerken, regels voor controle op e-mails en internetgebruik van werknemers.** A&V-21, 2000.

Buitenhuis, R., Campen, N.G.M. van, Helden, W.J. van, Vries, H.H. de, **Bankverzekeraars en privacy, gegevensverwerking in financiële conglomeraten.** A&V-20, Registratiekamer, 2000.

Helden, W.J. van, **Herkomst van de klant, privacyregels voor etnomarketing.** A&V-19, Registratiekamer, 2000.

Wishaw, R.W.A., **De gewaardeerde klant, privacyregels voor credit scoring.** A&V-18, Registratiekamer, 2000.

Artz, M. en Eijk, M.M.M. van, **Klant in het web, Privacywaarborgen voor internettoegang.** A&V-17, Registratiekamer, 2000.

Zeeuw, J. de, **Informatieverstrekking door de fiscus, Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving.** A&V-16, Registratiekamer, 1999.

Hes, R., Borking, J.J. en Hooghiemstra, T.F.M., **At face value, On biometrical identification and privacy.** A&V-15, Registratiekamer, 1999.

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

Borking, J.J., Eck, B.M.A. van en Siepel, P., **Intelligent software agents and privacy,** A&V-13, Registratiekamer, 1999.

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

Hes, R. en Borking, J., **Privacy-Enhancing Technologies: The path to anonimity. Revised Edition.** A&V-11, Registratiekamer, 1998.

Borking, J.J., Artz, M. en Almelo, L. van, **Gouden bergen van gegevens, Over datawarehousing, datamining en privacy,** A&V-10, Registratiekamer, 1998.

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

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

Ippel, P.C., **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.

Rossum, H. van e.a., **Privacy-Enhancing Technologies: the path to anonymity,** *volume I and II* A&V-5, Registratiekamer, 1995.

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

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

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

Hulsman, B.J.P. en Ippel P.C., **Personeelsinformatie-systemen, de Wet persoonsregistraties toegepast** A&V-1, Registratiekamer, 1994.

Overige publicaties

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

Persoonsgegevens beschermd, Uitspraken van de Registratiekamer, Sdu Uitgevers, Den Haag 1999, 69.

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

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

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

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

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

Rossum, H. van e.a., **Beveiliging van persoons-registraties,** Registratiekamer, 1994.

Brochures en Informatiebladen

Bijlage 5

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

Brochures

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

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

Registratiekamer, Registratiekamer 1999.

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

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

Informatiebladen

Verschillen tussen de Wet persoonsregistraties en de Wet bescherming persoonsgegevens, Registratiekamer 2000.

Als de politie u vragen stelt over uw klanten, Registratiekamer 1999.

Uw klacht en de Registratiekamer, Registratiekamer 1999.

Bemiddeling door de Registratiekamer, Registratiekamer 1999.

Het toetsen van uw kredietwaardigheid, Registratiekamer 1999.

Het gebruik van kentekengegevens en uw privacy, Registratiekamer 1999.

Camera's op de werkplek, Registratiekamer 1999.

Doorgeven van personeelsgegevens, Registratiekamer 1999.

Geadresseerde reclame, Registratiekamer 1999.

Publicaties in vakbladen en tijdschriften 2000

Bijlage 6

Berichten van de Registratiekamer in Privacy & Informatie, Koninklijke Vermande, Lelystad, 2000

Berichten van de Registratiekamer in Computerrecht, Amsterdam, 2000

Alonso Blas, D.M., **Privacy and the use of databases in forensic disciplines: a balance of interests,** Harmonisation in forensic expertise: *An inquiry into the desirability of and opportunities or international standards,* Criminal Sciences, Nijboer, J.F. and Sprangers, W.J.J.M. (editors), Thela Thesis, Amsterdam, 2000 blz. 499-511

Alonso Blas, D.M., **Universal effects of the European Datat Protection Directive,** A decade of research @ the crossroads of law and ICT, Dumortier, J., Robben, F. and Taeymans, M. (editors), Larcier, Brussel, 2000 blz. 23-33

Artz, M., **Technologie en privacy: Hand in hand of gezworen vijanden?,** Recht & Electronische Media, Kluwer, Deventer, nr. 4, januari 2000

Borking, J.J., **Erwartungen an die Datenschutz-beauftragten im internet** in het boek E-Privacy, *Datenschutz im Internet,* H. Bäumler (red.), Braunschweig/Wiesbaden, 2000

Borking, J.J., **Privacy Incorporated Software agents: A proposal for building a privacy guardian for the electronic age** in Privacy Law & Policy reporter Vol 7, no 5, november 2000

Hes, R. en Hooghiemstra, T.F.M., **Biometrie: meer dan persoonsherkenning,** i&i, Otto Cramwinckel, Amsterdam, nr.1 2000 blz. 35-41

Hooghiemstra, T.F.M. en Vries, H.H. de, **Werken met de WBP,** Nederlands Tijdschrift voor Sociaal Recht, Kluwer, Deventer, 2000 blz. 34-40

Hooghiemstra, T.F.M., **ICT en het medisch dossier,** J. Legemaate et. Al 'Knelpunten rond het medisch dossier, Koninklijke Vermande, Lelystad, februari 2000

Hooghiemstra, T.F.M., **Labaratoriumuitslagen en databescherming,** Nederlands Tijdschrift voor Klinische Chemie 2000, 25, nr. 4, blz 259-262

Linden, A. ter en Schreijnders R., **Medische chipkaart: pas op de plaats. Zijn privacy en beroepsgeheim nog wel gegarandeerd?,** Praktijkmanagement, Mediselect BV, Leusden, 2000 blz. 71-74

Pol, U. van de, en Stratum, M. van, **Wet bijzondere politieregisters bezien,** Nederlands Juristenblad, Kluwer, Deventer, 2000 blz. 215 t/m 219

Pol, U. van de, **(op)sporen op internet; privacy-bescherming onder druk,** Rede en recht, liber amicorum Nico Keijzer, Deventer, 2000 blz. 303-320

Pol, U. van de en Vries, H.H. de, **De werknemer achtervolgd: checklist voor 'personeelsvolgsystemen' en registratie van persoonsgegevens,** Controle en privacy van werknemers, Nieuwe regels voor observatie en registratie van uw personeel, RPMS publishers bv, Amsterdam, 2000, blz 51-60

Pol, U. van de, **(op)sporen op internet; privacy-bescherming onder druk,** privacy & informatie, Koninklijke Vermande, Lelystad, 2000 blz. 148-152

Stratum, M. van, **Privacy en opsporing II,** Nederlands Juristenblad, Kluwer, Deventer, 2000 blz.

Terstegge, J.H.J., **Is uw PI-systeem WBP-proof?,** Personeelsinformatie nr. 1, februari 2000

Terstegge, J.H.J., **Kernbegrippen uit de Wet bescherming persoonsgegevens,** Controle en privacy van werknemers, Nieuwe regels voor observatie en registratie van uw personeel, RPMS publishers bv, Amsterdam, 2000, blz. 9-18

Versmissen, J.A.G. en Hes, R., **Sleutelen aan privacy,** i&i, Otto Cramwinckel, Amsterdam, nr. 2, 2000 blz. 22-27

Vries, H.H. de, **Hoe werkt informationele privacy,** Meer respect voor grondrechten van werknemers, Stichting FNV Pers, Utrecht, 10 januari 2000

Vries, H.H. de, **Hoe werkt informationele privacy?** Meer respect voor grondrechten van werknemers, Stichting FNV Pers, Utrecht, april 2000

Vries, H.H. de, **Privacyregels voor ziekteverzuim en reïntegratie,** Controle en privacy van werknemers, Nieuwe regels voor observatie en registratie van uw personeel, RPMS publishers bv, Amsterdam, 2000 blz. 29-38

Vries, H.H. de, **Vertrouwelijkheid van e-mail op het werk,** Privacy & Informatie, Koninklijke Vermande, Lelystad, 2000 blz. 163-168

Wishaw, R.W.A. en Rodrigues, P.R., **Het recht op privacy en gelijke behandeling bij selectie en acceptatie,** Privacy & Informatie, Koninklijke Vermande, Lelystad, 2000 blz. 106-113

Zandee, C.G. **De nieuwe Wet bescherming persoonsgegevens en de advocatenpraktijk,** *modernisering privacybescherming,* Advocatenblad, Sdu uitgevers, Den Haag, 2000 blz. 939-945

Gedragscodes

Bijlage 7

Gedragscodes waarvoor de Registratiekamer een Verklaring van Overeenstemming heeft verleend

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

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

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

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

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

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

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

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

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

Gedragscode van het Nationaal Chipcard Platform, geldig tot 18 september 2001 (Stcrt. 1996,195)

Modelreglementen vastgesteld voor politieregisters

Bijlage 8

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)
Bureau Financiële Ondersteuning (Stcrt. 1996,125)
Fraudebestrijding (Stcrt. 1994,78)
Gevonden en verloren goederen (Stcrt. 1994,78)
Graffitibestrijding (Stcrt. 1994,78)
Herkenningsdienst (Stcrt. 1994,78)
Inbeslaggenomen goederen (Stcrt. 1994,78)
Inbraakbestrijding (Stcrt. 1994,78)
In bewaring genomen goederen (Stcrt. 1994,78)
Informantenregister (Stcrt. 2000, 198)
Internationale rechtshulp politie (Stcrt. 1994,144)
Jeugd- en zedenzaken (Stcrt. 1994,78)
Kabinetszaken (Stcrt. 1994,78)
Meldkamer (Stcrt. 1994,78)
Milieudelicten (Stcrt. 1994,78)
Multipol (Stcrt. 1994,78)
Openbare orde Regionale inlichtingendienst (Stcrt. 1996,125)
Opkopers en Helingbestrijding (Stcrt. 1994,78)
Overvallenbestrijding (Stcrt. 1994,78)
Permanent Autoteam (Stcrt. 1994,78)
Processen-verbaal en rapporten (Stcrt. 1994,78)
Recidive (Stcrt. 1994,78)
Rijverboden (Stcrt. 1994,78)
Schietwapen incidentenregistratie en informatiesysteem (Stcrt. 1994,78)
Technische recherchezaken (Stcrt. 1994,78)
Vakantiecontrolekaarten (Stcrt. 1994,78)
Vandalismebestrijding (Stcrt. 1994,78)
Verdovende middelen (Stcrt. 1994,78)
Voorlopig register (Stcrt. 2000,198)
Wijziging Herkenningsdienst (Stcrt. 1996,125)
Zware Criminaliteit (Stcrt. 2000,198)

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

Bijlage 9

21 November 2000 – **Privacy on the Internet – An integrated EU Approach to On-line Data Protection** (Document 5063/00-WP 37)

2 November 2000 – **Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 – COM (2000) 385** (Document 5042/00-WP 36)

13 July 2000 – **Opinion 6/2000 on the Human Genome and Privacy** (Document 5062/00-WP 34)

13 July 2000 – **Opinion 5/2000 on The Use of Public Directories for Reverse or Multi-criteria Searching Services (Reverse Directories)** (Document 5058/00-WP 33)

16 May 2000 – **Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"** (Document 434/00-WP 32)

16 March 2000 – **Opinion 3/2000 on the EU/US dialogue concerning the "Safe harbor" arrangement** (Document 5019/00-WP 31)

3 February 2000 – **Recommendation 1/2000 on the Implementation of Directive 95/46/EC** (Document 5139/00-WP 30)

3 February 2000 – **Opinion 2/2000 concerning the general review of the telecommunications legal framework** (Document 5009/00-WP 29)

3 February 2000 – **Opinion 1/2000 on certain data protection aspects of electronic commerce** (Document 5007/00-WP 28)

Zie ook:
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

Financiën 1999-2000

Bijlage 10

	Budgettoekenning (x f 1.000) 1999	%	(x f 1.000) 2000	%
Personeel	4869,0	77,4	5245,0	81,7
Materieel	1421,0	22,6	1178,0	18,3
Totaal	**6290,0**		**6423,0**	

Formatie 1999-2000

Bijlage 11

	1999	2000 man	vrouw
In dienst	15	4	6
Uit dienst	9	6	4
Bezetting einde jaar m/v		24	27
Bezetting einde jaar totaal	45,9	51,0	
Gemiddelde bezetting in fte's	47,9	47,8	
Toegewezen formatie in fte's	49,4	49,4	

Overige personele informatie 1999-2000

Bijlage 12

	1999	2000
Ziekteverzuim exclusief zwangerschap	9%	8%
Waarvan langdurig	5%	4%
Ouderschapsverlof	0	2
Zwangerschaps- en bevallingsverlof	0	2
Kinderopvangplaatsen gekocht	3	2
Opleiding/training (x 1.000 gulden)	69,5	87,4

Activiteiten 1997-2000 in cijfers

Bijlage 13

	1997	1998	1999	2000
Adviezen aan regering en parlement	27	18	13	23
Rapporten	7	9	16	4
Achtergrondstudies en Verkenningen	0	6	4	6
Overige publicaties	1	1	1	0
Klachten en geschillen	374	319	276	323
Telefonisch spreekuur	4.790	5.500	6.763	8.907
Aanmeldingen	57.786	61.111	63.400	65.977
Schriftelijke verzoeken om advies	517	595	687	910

Colofon

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

Samenstelling & eindredactie:
Rudy Schreijnders

Fotografie:
Karin van Kooten

Druk:
Sdu Grafisch Bedrijf bv

Vormgeving:
Miriam Monster (Proforma)

Met bijzondere dank aan:
Diana Alonso Blas, Gilles van Blarkom,
Erica Bool-Houwen, Maartje van Eijk,
Anne-Marije Fontein, Theo Hooghiemstra,
Bernard Hulsman, Linda van Laviere,
Jan-Paul Leerentveld, Elly Romanesko,
Anne Smeets, Michel van Stratum,
Richard Wishaw en Carine Zandee.