2003 in vogelvlucht

privacybescherming is een grondrecht, maar daarmee nog geen absoluut
: recht behoort de zorgvuldige omgang met persoonsgegevens. Het hierin
ng zal steeds afgewogen moeten worden tegen andere belangen. In de
tor vindt deze belangenafweging in laatste instantie plaats in het parlement
ich doorgaans in waarborgen voor de burger bij het verzamelen en gebruiken
oonsgegevens. Burgers kunnen zich vaak in een dergelijke afweging vinden.
alen van de balans liggen immers authentieke belangen. Het dient echter
elang van burgers in een democratische rechtsstaat als overheidsinstanties
net persoonsgegevens kunnen omgaan. Een democratische belangenafweging
k te resulteren in een zorgvuldige en systematische omgang met persoons-
n burgers door de overheid. Het CBP is bezorgd over de erosie in de publieke
n het fundamentele en in internationale verdragen vastgelegde beginsel dat
van persoonsgegevens dan wel het maken van een inbreuk op de persoonlijke
verkelijk noodzakelijk moet zijn.

Noodzakelijkheid als leidraad

Van erosie van het noodzakelijkheidsbeginsel is sprake als politici, ambtsdragers en beleidsmakers zich niet langer de vraag stellen of het verzamelen, gebruiken en bewaren van gegevens van burgers noodzakelijk is voor een bepaald doel. Het feit dat instanties nu eenmaal beschikken over veel gegevens van burgers is op zich geen toereikende legitimatie om deze voor andere doeleinden aan te wenden, langdurig te bewaren of met andere organisaties te delen.

Deze toets aan de noodzakelijkheid laat ruimte voor het gebruik van een basisset van gegevens van burgers door diverse overheidsinstanties en daarmee verwante instellingen. Ook samenwerking tussen instanties is zeer wel mogelijk, mits daarbij telkens weer wordt vastgesteld welke gegevensuitwisseling noodzakelijk is voor de samenwerking en mits de betrokken burger goed wordt geïnformeerd. Complexer wordt de situatie bij publiek-private taakverdeling. Met name bij de overheveling of uitbesteding van onderdelen van de sociale zekerheid dient uitdrukkelijk aandacht te worden besteed aan het juiste gebruik van (veelal bijzondere) persoonsgegevens door de marktpartijen. Uitbesteding ontslaat de overheid niet van haar eigen verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens.

Controle, veiligheid en vrijheid

In het publieke debat klinkt aanhoudend de roep om meer controlemaatregelen. Nuchtere afweging en realistische taxatie van het effect van voorgestelde maatregelen lijken te bezwijken onder de reële dreiging van terroristische aanslagen en de last van ernstige criminaliteit. De symboliek van voorstellen is echter vaak vele malen groter dan de effectiviteit ervan. Steeds verder gaande controlemaatregelen zullen echter niet zonder meer leiden tot vergroting van de veiligheid van de burger, terwijl de maatschappelijke kosten voor overheid en burgers hoog zijn. Een doorslaande zorg om veiligheid zal op den duur de vrijheid van de burger aantasten.

Bezinning op nut, noodzaak en maatvoering van te nemen controlemaatregelen is nodig. Maatregelen kunnen ook tijdelijk zijn; de reikwijdte ervan kan beperkt worden tot plaatsen of tijden met een verhoogd risico. Evaluatie van de maatregelen zou standaard moeten zijn, zeker bij ingrijpende controlemiddelen zoals cameratoezicht, preventief fouilleren en identiteitscontroles. Doordachte maatregelen, een proportionele inzet en het meten van effectiviteit bij het bestrijden van terrorisme en andere vormen van ernstige criminaliteit passen een overheid die de hoeder is van onze grondrechten.

Privacy van meet af aan

Bij het aantreden van het nieuwe kabinet in 2003 heeft het CBP aandacht gevraagd voor een zorgvuldige omgang met persoonsgegevens. Op tal van punten – zorg, veiligheid, fraudebestrijding en elektronische overheidsdienstverlening – raakt het kabinetsbeleid immers aan een zorgvuldige en behoorlijke verwerking van persoonsgegevens. Als privacybescherming veronachtzaamd wordt, ontstaan aanzienlijke risico's voor de houdbaarheid in rechte van beleidsinitiatieven en overheidsoptreden. Grotere speelruimte voor succes wordt gewonnen door van meet af aan privacybescherming mee te nemen bij het ontwerp van maatregelen en informatiesystemen.

Bij voorstellen voor wet- en regelgeving die in belangrijke mate betrekking hebben op de verwerking van persoonsgegevens, dient het CBP om advies gevraagd te worden. In overleg met de departementen zijn in 2003 betere voorwaarden geschapen voor de invulling van deze verplichting.

Informatie-infrastructuur

Stroomlijning van basisgegevens dient niet uit te monden in ongebreideld verkeer van persoonsgegevens binnen de overheid. Voor grote gegevensstromen is een specifieke en duidelijke wettelijke regeling geboden, met aandacht voor onder meer de maatschappelijke noodzaak, rol- en taakverdelingen, het feitelijke gegevensverkeer en transparantie.

In 2003 werd vervolg gegeven aan het advies *Persoonsnummerbeleid* van de zogenaamde Tafel Van Thijn over het inrichten van een overkoepelende informatie-infrastructuur voor de overheid. Bij de ontwikkeling van een plan voor de invoering was het CBP zowel op stuurgroep- als op werkgroepniveau intensief betrokken. Het CBP heeft onder meer een bijdrage geleverd aan de voorstellen voor een Nationale Vertrouwensfunctie, een organisatie die tot taak zal krijgen de burger inzicht te geven in alle gegevensstromen op basis van het burgerservicenummer. Vertrouwen van de burger in de elektronische overheid is essentieel. Het CBP zal daarom bestaande en nieuwe gegevensverwerkingen toetsen en in de toekomst een ombudsfunctie op dit terrein vervullen.

Gemeenten

De gemeente is voor de burger een belangrijke overheid waarmee hij veel te maken heeft. Gemeenten verwerken daarom ook veel persoonsgegevens van burgers. Door ontwikkeling in de taken en het bestuur van de gemeente neemt de verantwoordelijkheid voor de bescherming van persoonsgegevens nog toe. Het is daarom van groot belang dat gemeenten hun informatiehuishouding op orde hebben, ook ten behoeve van de bescherming van de persoonsgegevens van hun ingezetenen.

Resultaten 2003

In het vorige jaarverslag is aangekondigd dat in 2003 zou worden gestreefd naar de volgende resultaten:

- **Wetgevingsadviezen**
  Ingevolge artikel 51 lid 2 WBP moet het CBP om advies worden gevraagd 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 CBP heeft bij vrijwel alle departementen aandacht gevraagd voor de adviesplicht en afspraken kunnen maken zodat op adequate wijze invulling kan worden gegeven aan deze verplichting.

- **Functionarissen gegevensbescherming**
  Het aantal functionarissen voor de gegevensbescherming (FG), dat bij het CBP werd aangemeld op grond van de artikelen 62-64 WBP, groeide met 51 tot 148 eind 2003. Het CBP droeg bij aan de organisatie van een contactdag voor FG's werkzaam bij gemeenten en alle FG's hebben een contactpersoon binnen het CBP. Het samenspel tussen de toezichthouder en de functionarissen voor de gegevensbescherming is in ontwikkeling.

- **Cameratoezicht**
  Het CBP publiceerde in 2003 de resultaten van het onderzoek naar de wijze waarop bij Nederlandse gemeenten het cameratoezicht op openbare plaatsen in de praktijk functioneert en hoe met de privacyaspecten daarvan in verschillende gemeenten wordt omgegaan: *Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten.*

- **Zieke werknemer**
  Al enkele jaren wordt getracht de instroom van zieke werknemers in de WAO te beperken. Dit heeft geleid tot een toenemende behoefte aan informatie over de zieke werknemer die direct raakt aan diens privacy. Het CBP heeft in 2003 het onderzoek afgerond naar de privacyaspecten van de complexe regelgeving en de belangrijkste gegevensstromen omtrent de zieke werknemer. De publicatie van de studie is vertraagd.

- **Politieregisters**
  In het verlengde van eerdere activiteiten met betrekking tot de registers van de Criminele Inlichtingeneenheden (CIE's), is het CBP gestart met een steekproefsgewijze doorlichting van de praktijk bij 8 van deze eenheden. In de geselecteerde dossiers werd onderzocht in hoeverre de regels voor de informatieverwerking daadwerkelijk waren gevolgd. Het onderzoek zal in 2004 worden afgerond.

Bij analyse van de eerste 13.000 meldingen van verwerkingen van persoonsgegevens onder de Wet bescherming persoonsgegevens (WBP) bleek dat onder meer bij gemeenten het aantal meldingen sterk achterbleef bij de verwachtingen; zeker 60 gemeenten bleken de meldingsplicht consequent te negeren. In een steekproef heeft het CBP vervolgens bij een aantal gemeenten gecontroleerd of zij voldaan hadden aan de meldingsplicht. In december 2003 is aan een eerste gemeente een boete opgelegd voor het niet nakomen van de meldingsplicht.

Cameratoezicht door gemeenten

Bij alle gemeenten heeft het CBP in 2003 een onderzoek laten verrichten naar de inzet van cameratoezicht. Doel van het onderzoek *Cameratoezicht in de openbare ruimte* was een overzicht te verkrijgen van de wijze waarop cameratoezicht in de praktijk functioneert en hoe met de privacyaspecten van cameratoezicht in de verschillende gemeenten wordt omgegaan. Uit het onderzoek bleek dat één op de vijf gemeenten camera's inzet voor openbare orde, toezicht en veiligheid. Meer dan de helft van de gemeenten met cameratoezicht heeft echter de effectiviteit ervan niet geëvalueerd. Ruim de helft van de gemeenten benut het cameratoezicht in het kader van samenwerking tussen instanties en organisaties. Meestal gaat het om samenwerking met de politie bij opsporing, maar ook samenwerking met bedrijven en andere organisaties komt regelmatig voor. De kaders waarbinnen dit gebeurt, bleken echter vaak niet duidelijk.

Rotterdam: Persoonsgebonden aanpak mogelijk

Eind 2002 bestreed het CBP de opvatting van het stadsbestuur van Rotterdam dat aanpassing van de privacywetgeving nodig was voor een veilige stad.

- **Telecommunicatie**
  Het CBP heeft aandacht besteed aan de meldingsplicht binnen de telecommunicatiesector en adviseerde over de nieuwe Telecommunicatiewet. Eind 2003 heeft het CBP de sector schriftelijk geconsulteerd inzake nummeridentificatie met het oog op een verheldering van de normen voor de praktijk.

- **Certificering**
  Op basis van de uitkomsten van het eerdere project Auditaanpak is de grondslag gelegd voor een systeem van privacycertificering. Doel hiervan is de naleving van privacywetgeving via zelfregulering verder te bevorderen. In samenwerking met de toekomstige accreditatie-instellingen NOREA en NIVRA heeft het CBP dit systeem in 2003 vrijwel gereed gemaakt voor invoering.

- **Meldingsplicht**
  De verplichting om verwerkingen van persoonsgegevens bij het CBP te melden, draagt bij aan transparantie en controleerbaarheid. Op basis van het openbaar register heeft het CBP in 2003 een analyse van de meldingen uitgevoerd met het oog op de handhaving van deze verplichting. Uiteindelijk is in een drietal sectoren en bij de gemeenten nader onderzoek ingesteld dat eind 2003 heeft geleid tot de eerste bestuurlijke boetes.

- **Internetsite**
  De toegankelijkheid van de CBP-website is verbeterd, onder meer door de introductie van themadossiers en een nieuwsbrief via e-mail. De groeiende omvang van de website en de noodzaak het beleid inzake de nieuwe taken van het CBP inzichtelijk te maken, leidden ertoe dat in 2003 begonnen is met een herontwerp van de website. De voorgenomen aparte sectie voor praktische vragen van betrokkenen is niet gerealiseerd en zal worden meegenomen in het herontwerp.

- **Formatieplan**
  Om een goede uitvoering van nieuwe taken op het terrein van toezicht en handhaving te kunnen verzekeren, zijn de organisatie en formatie van het CBP aangepast. Op basis van het nieuwe formatieplan functioneert sinds 1 januari 2003 de afdeling Interventie, bezwaar en beroep. De vernieuwing van de organisatiestructuur kon in 2003 worden afgerond met de oprichting per 1 januari 2004 van de afdeling Onderzoek. De bijbehorende functieprofielen werden voor zover mogelijk in 2003 gerealiseerd.

'Smoelenboek'

Het komt regelmatig voor dat de politie bestanden aanlegt van personen zonder de directe aanleiding van een strafbaar feit maar wel met een concreet doel. Het gaat om (digitale) verzamelingen van persoonsgegevens waarmee mensen te herkennen zijn, meestal foto's met naam, adres, persoonsbeschrijvingen. Deze gegevens waren al opgenomen in een politieregister en worden dan opnieuw gebruikt. Zo'n bestand wordt in de politiepraktijk een 'smoelenboek' genoemd en het wordt in de regel gemaakt voor een beperkte groep van opsporingsambtenaren, bijvoorbeeld voor een wijkteam.
Het aanleggen van zo'n bestand mag. Er is zelfs een modelreglement op van toepassing, het reglement Aandachtsvestigingen. In 2003 adviseerde het CBP alle korpsbeheerders hierover. Privacywetgeving vereist dat er voldoende waarborgen zijn voor de kwaliteit van een smoelenboek. Rechtmatigheid vanuit het oogpunt van privacy en bruikbaarheid voor de politietaak liggen hier in elkaars verlengde. Een ongerichte collectie gegevens helpt op straat niet, een duidelijk doel en heldere selectiecriteria leveren wel een effectief instrument op. Privacynormen vereisen voor het verzamelen van persoonsgegevens eveneens een goed omschreven doel; duidelijke selectiecriteria zijn vereist om te voorkomen dat meer gegevens worden verwerkt dan noodzakelijk. Belangrijk zijn verder de actualiteit van de gegevens, digitale opslag in verband met een goed beheer en een beperking aan de duur dat de gegevens in het smoelenboek worden opgenomen.
Een bruikbaar digitaal smoelenboek van bijvoorbeeld de meest actieve autokrakers kan worden samengesteld op van grond van concrete selectiecriteria. Om te beginnen moet het gaan om een bepaald gebied, bijvoorbeeld een wijk. Verder moet de persoon blijkens de politieregisters meer dan tien keer verdacht zijn geweest van diefstal uit een auto door middel van braak. Deze diefstallen vonden plaats in het betreffende gebied in het tijdsbestek van de afgelopen 24 maanden. Indien bekend wordt ook de zogenaamde 'modus operandi' opgenomen, de typische manier van werken van de betreffende autokraker, bijvoorbeeld inbraak via de achterklep van de auto. Via autorisatie wordt deze selectie alleen beschikbaar gesteld aan een specifieke groep opsporingsambtenaren, in dit geval een wijkteam. Vervolgens wordt elke drie maanden gekeken of de personen nog rechtmatig in het smoelenboek staan. Deze waarborgen voor 'de privacy' zijn ook waarborgen voor de bruikbaarheid van het smoelenboek in de politiepraktijk door de duidelijke selectiecriteria en het actueel houden van de gegevens ●

In vervolg hierop heeft het CBP in 2003 overleg gevoerd met de partijen die betrokken zijn bij de diverse projecten voor een integrale aanpak van circa 700 drugsverslaafden die voor overlast zorgen of crimineel gedrag vertonen en doorgaans ook medische zorg en sociale hulp mijden. Aan dit samenwerkingsverband nemen onder meer deel de politie, de hulpverlening en de reclassering. Van de betrokken verslaafden worden gegevens over hun contacten met zowel de politie als de hulpverlening uitgewisseld. De gedeelde informatie wordt opgeslagen in een basisdossier. Op basis van het dossier wordt vervolgens besloten tot een bepaalde aanpak, de zogenaamde zorg-, drang- of dwangtrajecten.

De discussie binnen het samenwerkingsverband spitste zich toe op de grenzen die het beroepsgeheim van de zorgverleners stelt. Het CBP heeft in het overleg erop gewezen dat zorgverleners dienen vast te houden aan hun wettelijke plicht te handelen in het belang van de cliënt. Indien het naar hun professionele oordeel in het belang van de cliënt is dat zij informatie delen met andere instanties, is dat in principe mogelijk. Deze benadering gaf aanleiding tot een breder debat over de reikwijdte van het medisch beroepsgeheim onder regie van de Inspectie voor de Gezondheidszorg. In de loop van 2003 hebben de betrokken partijen de regels voor de informatie-uitwisseling uitgewerkt en kon het Informatiesysteem PGA gemeld worden bij het CBP.

Onvoldoende toezicht op uitvoering WWB

De kern van de nieuwe Wet werk en bijstand (WWB) is dat gemeenten meer (financiële) verantwoordelijkheid krijgen voor de bijstandsverlening. Het CBP heeft zich in 2002 en in 2003 meerdere malen uitgesproken over de inrichting van het toezicht op de uitvoering van de WWB. Er is een kloof tussen de formele regeling dat de Inspectie Werk en Inkomen (IWI) toeziet op de rechtmatigheid van de uitvoering (inclusief de verwerking van persoonsgegevens) en de praktische uitwerking waarin het IWI niet de nodige informatie ontvangt om structureel toezicht uit te oefenen. Deze kloof is niet gedicht bij de behandeling van het wetsontwerp in de beide Kamers. De uitwerking van het toezicht is voor wat betreft de verwerking van (persoons)gegevens verder niet in overeenstemming met het standpunt van de staatssecretaris van Sociale Zaken en Werkgelegenheid tijdens de parlementaire behandeling. Het CBP maakt zich zorgen over dit gebrek aan verantwoordingsplicht voor de gemeenten.

Politie en privacy

De bijdrage van een aantal hoofdcommissarissen aan de publieke discussie over veiligheid was niet in balans. Privacybescherming werd bij herhaling als obstakel voor het politiewerk, als belemmering voor betere resultaten aangewezen. Toonaangevende politiemensen leken te miskennen dat de politie kan beschikken over zeer veel bronnen van informatie over burgers. Privacybescherming verplicht de politie daarmee op verantwoorde en controleerbare wijze om te gaan. De typering van het grondrecht op privacy als 'schuilplaats van het kwaad' door de korpschef van Groningen was ver over de schreef.

Het CBP onderkent dat de politie een grote en legitieme informatiebehoefte heeft en kon zich op hoofdlijnen vinden in de voorgenomen uitbreiding van de bevoegdheid van justitie en politie om persoonsgegevens op te vragen bij maatschappelijke instellingen en bedrijven als dat voor de opsporing noodzakelijk is. Het wetsvoorstel is gebaseerd op de voorstellen van de commissie Mevis (2001) en schept vooral duidelijkheid voor het bedrijfsleven. Naar het oordeel van het CBP is wel een contragewicht nodig. Niet alleen dient informatie gericht en selectief verzameld en gebruikt te worden, maar er dient ook toezicht op de informatiehuishouding van de politie te zijn, onder andere in de vorm van periodieke en onafhankelijke controles achteraf. De minister van Justitie heeft dit ook toegezegd in het kabinetsstandpunt over de voorstellen van de commissie Mevis. Het CBP heeft aangedrongen op een spoedige invoering van deze periodieke audits op alle politieregisters.

Criminele inlichtingeneenheden

In 2003 is het CBP begonnen met een eerste serie onderzoeken bij de criminele inlichtingeneenheden (CIE's) van acht politiekorpen in aanvulling op de door de politie georganiseerde zelfevaluatie en onafhankelijke review van 2002. CIE's voeren een aantal bijzondere registers, die ook opsporingsinformatie over niet-verdachte personen bevatten. Onafhankelijk, extern toezicht is daarom van wezenlijk belang. Alleen het CBP kan als externe toezichthouder kennisnemen van de inhoud van de dossiers. Bij deze serie onderzoeken ging het om steekproefsgewijze doorlichting van de praktijk. In de geselecteerde dossiers werd onderzocht in hoeverre de regels voor de informatieverwerking daadwerkelijk waren gevolgd. In 2004 zullen de onderzoeken worden afgerond.

Advocaten afgeluisterd

Uit het CBP-onderzoek naar het afluisteren en registreren van gesprekken van burgers met hun advocaten bleek dat het beroepsgeheim van advocaten onvoldoende gerespecteerd werd. Het stelselmatig opnemen, registreren, uitwerken en kennisnemen van deze vertrouwelijke communicatie door de politie en het Openbaar Ministerie is strijdig met de bij wet en verdrag erkende bijzondere positie van beroepsgeheimhouders. Het is daarmee ook in strijd met de Wet politieregisters en de Wet bescherming persoonsgegevens. Politie en justitie waren doorgeschoten bij het afluisteren en registreren van gesprekken van burgers met hun advocaten. De minister van Justitie deelde het standpunt van het CBP echter niet en heeft de aanbevelingen niet overgenomen.

Administratieve lastenverlichting

Het aantal verzoeken om kennisneming bij de politie door personen die willen weten of en hoe zij geregistreerd staan in politieregisters, was in voorgaande jaren aanzienlijk toegenomen. Het aantal verzoeken steeg van 1100 in 2000 tot 1850 in 2002. Het ging vooral om complexe en tijdrovende verzoeken van advocaten, die door een CIE worden behandeld. Een werkgroep van privacydeskundigen van de politie, het Openbaar Ministerie en het CBP kwam met een plan voor de stroomlijning van de behandeling van de verzoeken. Hiermee zal ook uitholling van het recht op kennisneming worden voorkomen.

Belangrijk in het kader van de administratieve lastenverlichting zijn ook de modelreglementen voor de politieregisters. In 2002 keurde het CBP 40 modelreglementen voor de permanente registers goed. In 2003 kwam het Modelreglement Tijdelijk register tot stand. Het gebruik van modelreglementen vermindert direct de administratieve lasten bij politie en CBP en schept tegelijkertijd waarborgen.

Marktwerking in de zorg

De discussie over kostenbeheersing en kwaliteitsversterking in de zorg wordt gedragen door een consensus over de noodzaak van meer marktwerking via publiek-private samenwerking waarbij voor de zorgverzekeraars zich een zeer

Een medisch dossier bij het UWV

Je wacht op een herbeoordeling voor een WAO-uitkering, je medische dossier bij het UWV – het Uitvoeringsinstituut werknemersverzekeringen – blijkt zonder je toestemming aan een andere arts van een extern bedrijf te zijn gegeven en het raakt ook een paar keer 'kwijt'. Niemand heeft je iets verteld of gevraagd. De klacht die het CBP hierover ontving, maakt twee dingen nog weer eens duidelijk. Overheid of bedrijfsleven kunnen alleen rekenen op vertrouwen als burgers goed geïnformeerd worden en dat vertrouwen is ook nodig om complexe maatschappelijke organisaties goed te laten draaien.

De verzekeringsartsen bij het UWV hadden met grote achterstanden te kampen zodat het onmogelijk was de schriftelijke herbeoordeling van alle dossiers uit te laten voeren door medewerkers van het UWV. Daarom werden verzekeringsartsen en arbeidsdeskundigen ingehuurd bij een bedrijf. Medische dossiers werden daarvoor ook op en neer gestuurd naar verschillende locaties in het land. Het is dan niet vreemd te denken dat je medische herbeoordeling zomaar is uitbesteed. De zaak lag echter toch anders.

Het UWV mag kerntaken – zoals het beoordelen van medische dossiers – immers niet uitbesteden aan private uitvoerders. Het UWV had daarom extra mensen ingehuurd bij een bedrijf waarmee ook een overeenkomst werd gesloten over de van toepassing zijnde geheimhoudingsplicht, het werken volgens kwaliteitsnormen en de naleving van het privacyreglement van het UWV. De ingehuurde deskundigen deden hun werk dus onder leiding en onder de voorwaarden van het UWV alsof zij medewerkers van het UWV waren.

prominente rol begint af te tekenen. De verzekeraars stellen echter dat zij zonder maximaal inzicht in de feitelijke, individuele zorg deze rol niet kunnen vervullen. Dit bleek in de discussie over de introductie van de Diagnose Behandeling Combinatie (DBC).

De DBC-systematiek is ontwikkeld voor de bekostiging van specialistische medische zorg en moet leiden tot een marktconforme prijsontwikkeling op basis van onderhandelingen tussen zorginstellingen en zorgverzekeraars. Een DBC is een combinatie van codes die gegevens bevatten over onder andere de zorgvraag, de diagnose en de behandeling van een patiënt. Op deze informatie is het medisch beroepsgeheim van toepassing. Zorgverleners dienen de DBC's te verstrekken aan zorgverzekeraars voor de declaratie van de verleende zorg.

Het CBP heeft zich sterk gemaakt voor het medisch beroepsgeheim en maatvoering bij de verstrekking van medische persoonsgegevens. Het CBP stond op het standpunt dat inzichtelijk moest worden gemaakt welke persoonsgegevens noodzakelijkerwijs door ziekenhuizen aan de zorgverzekeraars zouden moeten worden verstrekt. Als duidelijk is welke gegevensverwerkingen noodzakelijk zijn voor de diverse, gerechtvaardigde doeleinden, zou de juridische verankering van het nieuwe bekostigingssysteem daarop kunnen aansluiten.
De uitwerking van het noodzakelijkheidcriterium heeft geresulteerd in een toetsingskader. Dit biedt vijf criteria aan de hand waarvan bepaald wordt of een DBC al dan niet gedeclareerd zal worden met alle bijbehorende informatie over de diagnose.

De DBC-systematiek zal vanaf 1 januari 2005 gefaseerd ingevoerd worden. In een gezamenlijke brief hebben de minister van VWS en het CBP de betrokken partijen (zoals Zorgverzekeraars Nederland en koepelorganisaties) gevraagd de werkwijze voor de invoering van het stelsel onder de aandacht van hun leden te brengen.

De zieke werknemer

Al enkele jaren wordt getracht de instroom van zieke werknemers in de WAO te beperken. Dit heeft geleid tot maatregelen voor een actiever ziekteverzuimbeleid, strengere reïntegratieverplichtingen voor werknemer en werkgever en

Deze constructie – de gezagsverhouding en de overeenkomst – zorgde ervoor dat de verantwoordelijkheid voor het gebruik van de medische en andere persoonsgegevens in de uitkeringsdossiers bij UWV bleef, waar deze ook hoort. Hoe het werk door de verantwoordelijke georganiseerd wordt, is dan in principe een interne kwestie.
Maar was er dan geen toestemming nodig van de betrokkene voor de overdracht van het dossier aan een andere arts? Volgens de kwaliteitsrichtlijnen van UWV kan de verzekeringsarts alleen medische dossiers van andere verzekeringsartsen gebruiken voor zover hij hen opvolgt, voor hen waarneemt, of een bezwaarschrift behandelt. In dit geval kon naar het oordeel van het CBP gesproken worden van waarneming. De verzekeringsarts kon de schriftelijke beoordeling van het dossier immers niet zelf uitvoeren. Het vragen van toestemming aan de betrokkene was naar het oordeel van het CBP daarom ook niet verplicht. Het UWV had echter wel moeten zeggen dat voor heronderzoek het dossier aan een andere verzekeringsarts zou worden overgedragen. In dit geval werd immers afgeweken van wat de betrokkene redelijkerwijs had kunnen verwachten, namelijk een herbeoordeling door een arts die in dienst is bij de door de wet aangewezen instantie. Goede informatie had de betrokkene in staat gesteld hiertegen eventueel bezwaar te maken.
Het CBP kwam tot de conclusie dat het UWV heeft gehandeld in strijd met de Wet bescherming persoonsgegevens voor wat betreft de informatieplicht en de zorgvuldige omgang met het dossier. Het UWV hoefde echter geen toestemming aan de betrokkene te vragen voor de gang van zaken. Het UWV heeft ook maatregelen getroffen om het vervoer van de dossiers te verbeteren ●

Doelen 2004

In 2004 zullen met name de volgende resultaten worden nagestreefd:

- **Zieke werknemer**
  Het onderzoek naar de belangrijkste gegevensstromen omtrent de zieke werknemer en de daarbij behorende privacyregels zal in 2004 resulteren in de publicatie van een naslagwerk met vuistregels voor de praktijk. Het naslagwerk zal intensief onder de aandacht worden gebracht van de diverse bij reïntegratie van de zieke werknemer betrokken partijen.

- **Politieregisters**
  Het in 2003 gestarte onderzoek naar de registers van de Criminele Inlichtingeneenheden bij acht regiokorpsen zal in 2004 worden afgerond. De algemene bevindingen van het onderzoek zullen worden gepubliceerd.

- **Onderzoek tapkamers**
  Het CBP zal in 2004 een onderzoek instellen naar de privacy-aspecten van de gegevensverwerking in de tapkamers van de politie, dit in vervolg op het *Onderzoek naar de waarborging van de vertrouwelijke communicatie van advocaten bij de interceptie van telecommunicatie* uit 2003.

- **Cameratoezicht**
  De resultaten van het in 2003 gepubliceerde onderzoek *Cameratoezicht in de openbare ruimte. Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten* zullen in 2004 benut worden voor een studie over de privacyaspecten van cameratoezicht op de openbare ruimte waarin vuistregels gegeven zullen worden voor de praktijk.

- **Burgerservicenummer**
  Het CBP zal een bijdrage leveren aan het realiseren van de Nationale Vertrouwensfunctie, een organisatie die tot taak krijgt de burger inzicht te geven in alle gegevensstromen op basis van het burgerservicenummer. Het CBP zal in 2004 in de gelegenheid worden gesteld te beginnen met het toetsen van bestaande en nieuwe gegevensverwerkingen en zich voor te bereiden op een toekomstige ombudsfunctie.

- **Certificering**
  Het met NOREA en NIVRA uitgewerkte systeem van privacy-certificering dient in 2004 in de praktijk te worden gebracht, aanvankelijk in de vorm van proefcertificeringen, naderhand als marktproduct. Het CBP zal bijdragen aan de beoordeling van de proefcertificeringen.

- **Invoering DBC-systematiek**
  Op het gebied van de zorg zal het CBP nauw betrokken blijven bij de ontwikkeling en invoering van de financierings-systematiek op basis van de Diagnose Behandeling Combinatie.

- **Landelijke registraties in de zorg**
  In 2003 heeft het CBP een oriënterend onderzoek afgerond naar vijf landelijke registraties in de zorg. Het CBP zal de resultaten van het onderzoek in 2004 gebruiken voor de formulering van normen inzake landelijke registraties en het daarbij passende handhavingsbeleid.

- **Onderzoek privacybeleving**
  Het CBP zal een eerste onderzoek laten uitvoeren naar aspecten van privacybewustzijn en privacybehoeften bij de Nederlandse burger. Dergelijke onderzoeken zijn in verscheidene Europese landen reeds uitgevoerd. De resultaten zullen gebruikt worden bij het maken van strategische keuzes en de verdere invulling van het beleid van de toezichthouder.

- **Beleidsregels en tweedelijnspositie**
  Het CBP zal beleidsregels publiceren voor het in behandeling nemen van zaken en de publiciteit daaromheen. Ter uitvoering van het tweedelijnsbeleid zal het CBP sector-, branche-, koepel- en beroepsorganisaties benaderen om de mogelijkheden te onderzoeken van informatie-uitwisseling en taakverdeling bij voorlichting en klachtbehandeling.

- **Organisatieontwikkeling**
  In 2004 zal de afdeling Onderzoek operationeel moeten worden waarbij veel aandacht besteed zal worden aan differentiatie van onderzoeksvormen en de ontwikkeling van risico-analyse als instrument voor beleidsvorming. De afdeling speelt een belangrijke rol bij het voorgenomen onderzoek privacybeleving en is verantwoordelijk voor de meldingenanalyse 2004.

- **CBP-website**
  In 2004 zal het CBP zijn website vernieuwen met het oog op een betere voorlichting aan betrokkenen en verantwoordelijken. Het materiaal op de website zal meer vraaggericht ontsloten worden. Hiermee wordt ook een vermindering beoogd van de stroom van voorlichtingsverzoeken die het CBP telefonisch, per e-mail en per post jaarlijks bereiken.

Nevenfuncties van rechters

De burger heeft een groot belang bij een onafhankelijke en transparante rechterlijke macht. Informatie over nevenfuncties van rechters is daarom openbaar. Maar ook rechters hebben recht op privacy. Welke waarborgen kunnen worden getroffen om beide belangen in evenwicht te brengen? In 2003 heeft het CBP geadviseerd over de Wet nevenbetrekkingen rechterlijke ambtenaren evenals over de ermee samenhangende wijziging van de Wet rechtspositie rechterlijke ambtenaren.
Volgens het wetsvoorstel zou voortaan een nevenfunctie niet alleen gemeld moeten worden, maar zou ook worden beoordeeld of de nevenfunctie wel gewenst is. Gekeken wordt dan naar de goede vervulling van het ambt van rechter, diens onpartijdigheid en onafhankelijkheid of het vertrouwen daarin. Daarom moet ook de naam van het bedrijf of de instantie worden gemeld, het aantal uren per maand, de plaats en het moment van aanvang en beëindiging van de betrekking en of deze (on)bezoldigd is en de hoogte van de eventuele bezoldiging per jaar. Het wetsvoorstel regelt verder de (elektronische) openbaarmaking van deze gegevens. Deze aanscherping van de regeling past natuurlijk in de toegenomen aandacht voor de integriteit van ambtenaren en openbare ambtsdragers.
De onpartijdigheid en onafhankelijkheid van de rechterlijke macht vormen één van de essentiële verworvenheden van onze rechtsstaat. De inbreuk op de persoonlijke levenssfeer van rechterlijke ambtenaren was in de voorgestelde vorm dan ook te rechtvaardigen in het licht van de eisen die het Europese verdrag voor de rechten van de mens daaraan stelt. De openbaarmaking van al deze gegevens in een openbaar register was naar het oordeel van het CBP een minder uitgemaakte kwestie. De omvang en de verdiensten uit een nevenbetrekking kunnen van belang zijn voor de beoordeling van de verenigbaarheid van de nevenbetrekking met het rechtersambt. Vermelding van alle gegevens over de nevenbetrekking op een voor iedereen toegankelijke internetsite is echter voor deze beoordeling niet noodzakelijk. Dit kan door rechterlijke ambtenaren op goede gronden als een te vergaande inbreuk op hun persoonlijke levenssfeer worden ervaren. Het CBP adviseerde de volledige openbaarmaking te heroverwegen. In het openbaar register kan volstaan worden met het vermelden van de nevenfuncties ●

een langere verplichting voor de werkgever tot doorbetaling van het loon. Verder hebben ook andere organisaties en bedrijven een rol in het stelsel gekregen. Al deze partijen hebben een toenemende behoefte aan informatie over de zieke werknemer die direct raakt aan diens privacy.

Gezien de complexiteit van de regelgeving is het CBP in 2002 een onderzoek gestart naar de belangrijkste gegevensstromen omtrent de zieke werknemer en de daarbij behorende privacyregels. Eind 2003 kon het afgerond worden. Andermaal bleek hoe belangrijk het is dat de wetgever zorgt voor duidelijke regelgeving juist ook bij publiek-private samenwerking. Meer nog dan overheidsinstanties hebben bedrijven een belang bij duidelijkheid over wat wel en wat niet kan, zowel om redenen van bedrijfsvoering als omwille van reputatie en aansprakelijkheid.

Certificering van gegevensverwerkingen

In verschillende landen wordt gezocht naar manieren om concurrentie en marktwerking te benutten voor privacybescherming. Een van de mogelijkheden om in de markt zichtbaar te maken dat bedrijven en organisaties zich inspannen voor een zorgvuldige omgang met persoonsgegevens, is een privacycertificaat. Een aantal beroepsorganisaties heeft samen met het CBP een systeem ontwikkeld voor de private auditing van verwerkingen van persoonsgegevens. Het beoogde privacycertificaat kan worden toegekend aan een specifieke, rechtmatige verwerking van persoonsgegevens. Het certificaat is dus niet voor de organisatie in haar geheel. Het CBP zal in eerste instantie een tweetal accreditatie-instellingen benoemen, te weten NOREA en NIVRA voor het accrediteren van privacyauditors. In 2004 zal het systeem praktisch vorm krijgen.

Gedragscodes voor bedrijven

Bij de bescherming van persoonsgegevens is nadrukkelijk ruimte gecreëerd voor zelfregulering, onder meer door gedragscodes die zijn goedgekeurd door de toezichthouder. Gedragscodes zijn belangrijk, omdat de specifieke uitwerking van privacynormen voor een sector of beroep duidelijkheid schept voor de praktijk. Het CBP was betrokken bij het tot stand komen van gedragscodes voor financiële instellingen, de gerechtsdeurwaarders en de eerste Europese gedragscode voor direct marketing.

De begin 2004 goedgekeurde Privacygedragscode sector particuliere onderzoeksbureaus is opgesteld door de Vereniging van Particuliere Beveiligingsbureaus (VPB) en bindt de bij de VPB aangesloten bureaus. De particuliere recherche is een sterk groeiende sector waarvoor weinig geregeld was. De minister van Justitie is voornemens, in het kader van de vergunningverlening aan deze bureaus, de naleving van de gedragscode verplicht te stellen voor alle particuliere recherchebureaus. De minister van Justitie en het CBP hebben een overeenkomst gesloten om het toezicht op de branche af te stemmen.

Ook de Gedragscode inzake het verwerken van persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus (NVH) kon worden goedgekeurd. Juist in deze sector moest het CBP in de afgelopen jaren constateren dat er op grote schaal onzorgvuldig werd omgegaan met de bescherming van persoonsgegevens. Het CBP zal de gedragscode van de NVH hanteren als richtsnoer bij het toezicht op alle handelsinformatiebureaus.

Dwangsom voor handelsinformatiebureau X

In 2003 publiceerde het CBP de resultaten van het onderzoek naar handelsinformatiebureau X. De conclusie was dat het bureau onrechtmatig, onbehoorlijk en onzorgvuldig persoonsgegevens had verwerkt voor het maken van rapportages met verhaalsinformatie. Bij het Openbaar Ministerie werd aangifte

Pet past ons allemaal

Op 31 december 2003 werd het EU-project PISA succesvol afgesloten. In het project is beoogd aan te tonen dat persoonsgegevens ook met technologie beschermd kunnen worden door omzetting van wetgeving in computercode. Daarbij is gekozen voor een techniek waarbij software agents informatie uitwisselen in een internetomgeving in opdracht van hun eigenaar. Het gaat om software die zelfstandig beslissingen moet kunnen nemen. Opdrachten aan agents kunnen liggen in de sfeer van het boeken van de snelste reis of het reserveren van een restauranttafel, maar ook van het opvragen van belastinggegevens of medische informatie. Het kunnen vertrouwen op de technologie is in dergelijke gevallen noodzakelijk voor de acceptatie door het publiek, de overheid en het bedrijfsleven.

PISA staat voor Privacy Incorporated Software Agents en begon met een samenwerking tussen TNO-FEL en de Registratiekamer, de voorganger van het CBP, in 1999. In 2001 werd het een formeel project van de Europese Unie waarin naast TNO-FEL en het CBP ook TNO-TPD, de TU Delft, de National Research Council Canada, Sentient Machine Research, GlobalSign, Zeroknowledge en Finsa Consulting/Italsoft deelnamen.

Het CBP heeft de afgelopen jaren aan PISA bijgedragen, onder meer door de basisbegrippen van PET (Privacy-Enhancing Technologies) verder te verfijnen, door het ontwikkelen van een methodiek voor de omzetting van concepten uit de Europese Privacyrichtlijn 95/46 EG naar een metataal die gebruikt kan worden om computercode te schrijven en door hoofdstukken van de definitieve rapportage voor zijn rekening te nemen. Het CBP heeft in 2003 het eindrapport, Handbook of Privacy and Privacy-Enhancing Technologies, uitgegeven en zal in 2004 de finale privacyaudit uitvoeren. De materialen zijn beschikbaar via de website van het CBP.

PISA wordt afgesloten met de bottom line: "Privacy by design is achievable in even the most complex of applications" ●

gedaan van een vermoeden van een aantal strafbare feiten. Het opsporingsonderzoek heeft inmiddels geleid tot vervolging en berechting van enkele bij het bedrijf betrokkenen.

Het CBP had geconstateerd dat uit allerlei bestanden – waaronder die bij de Belastingdienst, uitkeringsinstanties en woningcorporaties – persoonsgegevens door het bureau onrechtmatig verkregen werden. Het CBP heeft daarom een groot aantal van deze instanties, bedrijven en beroepsorganisaties nader geïnformeerd over de bevindingen in het onderzoek, opdat zij passende maatregelen konden nemen. Een aantal van hen heeft daartoe relevante delen van het bewijsmateriaal ontvangen.

In mei 2003 legde het CBP bureau X een last onder dwangsom op. De last richtte zich op de naleving van twee punten waarop overtredingen van de WBP zijn geconstateerd: bureau X dient zich te onthouden van het verwerken van persoonsgegevens die onder geheimhoudingsverplichtingen vallen of waarvoor een verwerkingsverbod geldt en het bureau moet de betrokkene over wie persoonsgegevens worden verzameld, daarover inlichten.

Goede informatie voor de klant

Bedrijven hebben in beginsel ruime mogelijkheden om persoonsgegevens te verwerken voor marketingdoeleinden. Belangrijke voorwaarde voor een rechtmatige verwerking is goede informatie aan de klanten om wier gegevens het gaat. Transparantie is ook essentieel voor het vertrouwen van de klant. Dat bleek opnieuw in twee kwesties: het geheime nummer beleid van de KPN en de inrichting van een centrale database voor klantgegevens binnen de ING Groep.

ING Bank, Postbank en RVS – onderdelen van de ING Groep – hadden in 2002 een brief aan hun cliënten geschreven over het plan hun gegevens voor marketingdoeleinden voortaan ook in één centraal systeem vast te leggen. De geboden informatie gaf cliënten echter onvoldoende mogelijkheden hun rechten uit te oefenen. Na een onderzoek kwam het CBP tot de conclusie dat de bedrijven in deze onrechtmatig gehandeld hadden. Door de weinig specifieke wijze waarop de betrokkenen in de brief waren geïnformeerd over de gegevensverstrekking, was de verstrekking niet verenigbaar met het doel waarvoor de gegevens waren verzameld. De ING Groep had de cliënten van de diverse onderdelen beter moeten informeren om hun gegevens op centraal niveau verder te mogen verwerken. De klanten van ING Bank, Postbank en RVS hebben vervolgens aanvullende informatie gekregen.

Het CBP en de OPTA publiceerden medio 2003 het onderzoeksrapport over het beleid van Koninklijke KPN N.V. (KPN) omtrent nummers met beperkte bekendheid, algemeen bekend als ‘geheime nummers’. KPN bleek haar beleid halverwege de jaren ‘90 te hebben gewijzigd en stelt sinds geruime tijd de adresgegevens van abonnees met een geheim nummer voor direct marketing doeleinden aan derden ter beschikking zonder dat zij haar abonnees daarover expliciet heeft geïnformeerd. Het CBP verzocht KPN haar klanten actief te informeren over het beleid rond geheime nummers. Teleurstellend is dat de kwestie zich begin 2004 nog voortsleept, terwijl het in de kern gaat om een wettelijke plicht van het bedrijf om klanten te informeren over hun wettelijke rechten.