2002 in vogelvlucht

De politiek-maatschappelijke discussie draaide in 2002 vooral om veiligheid. In de algemene roep om meer daadkracht, toezicht en controle maakten diverse vooraanstaande bestuurders en politici van privacy een karikatuur. Privacybescherming zou meer veiligheid voor de burger in de weg staan; privacywetgeving moest daarom worden aangepakt. Het kabinet stelde in november voor een algemene identificatieplicht in te voeren voor alle burgers ouder dan 12 jaar. Met het oog op misdaad- en terrorismebestrijding zouden alle telecommunicatiegegevens van iedereen langdurig bewaard moeten blijven. Het CBP maakt zich ernstige zorgen over de gevolgen die een gemakzuchtige vlucht in meer politiebevoegdheden voor de belangen en rechten van gewone burgers kan hebben.

Het CBP maakt verder ernstig bezwaar tegen de suggestie dat juist privacybescherming de samenwerking van verschillende instanties bij het oplossen van maatschappelijke problemen zou belemmeren. Het is de overtuiging en de ervaring van het CBP dat privacybescherming een van de succesfactoren is voor een effectief overheidsoptreden. Privacyregels hoeven aan weinig legitieme overheidsdoelstellingen in de weg te staan. Wel dient vanaf het begin rekening met deze regels gehouden te worden, zowel bij het ontwerpen van organisatiestructuren, informatiesystemen en procedures als bij het opstellen van beleid.

Privacy en veiligheid

Het privacybelang van burgers wordt altijd afgewogen tegen andere zwaarwegende belangen. De Nederlandse grondwet, internationale verdragen, Europese richtlijnen en de privacywetgeving stellen eisen aan deze afweging. Dit maakt deel uit van de spelregels voor de overheid in de omgang met haar burgers. Privacyregels eisen dat goed wordt nagedacht over doel, effectiviteit en evenredigheid van overheidsmaatregelen en dat er voldoende waarborgen komen tegen misbruik. Wie de privacywetgeving op de helling wil zetten, zegt in feite dat deze vragen overbodig zijn.

Een onzorgvuldige omgang met de privacy van de burger stelt diens vertrouwen in de overheid op termijn in de waagschaal. Burgers die niets te verbergen hebben, verdienen een overheid die privacybescherming vanzelfsprekend meeneemt bij het ontwerp van maatregelen, informatiesystemen of verplichtingen voor burgers.

Het recht op 'privacy' is dus een essentieel onderdeel van de 'veiligheid' die een democratische rechtsstaat zijn burgers te bieden heeft. Wie het recht op privacy onderuit haalt, berooft de goedwillende burger van een belangrijke waarborg en zaagt aan de poten van de democratische rechtsstaat.

Identificatieplicht

In december 2002 werd een wetsvoorstel ontworpen voor een algehele identificatieplicht. Het CBP adviseerde begin 2003 het voorstel niet in te dienen. Het evenwicht tussen rechten en plichten voor burger en overheid is hier zoek. Burgers wordt een permanente verplichting opgelegd zonder motivering waarom specifieke verplichtingen niet voldoende zijn. Strafbaarstelling van het niet nakomen van de identificatieplicht leidt tot een situatie waarin iedere burger naar believen als verdachte kan worden bejegend.

De Nederlandse discussie over een beperkte of algemene identificatieplicht is zeker al twintig jaar oud. Steeds werd op goede gronden geconcludeerd dat een algemene identificatieplicht te ver ging. Aangezien in het voorstel ook geen nieuwe argumenten werden aangedragen, voldeed het kabinet niet aan de eis van het Europees Verdrag voor de Rechten van de Mens om de inbreuk op de persoonlijke levenssfeer voldoende te rechtvaardigen.

Cameratoezicht op openbare plaatsen

Publiek cameratoezicht blijft onverminderd in de belangstelling en zal wettelijk beter worden geregeld. Als middel om veiligheid en openbare orde te bevorderen werd het allerwegen geaccepteerd hoewel de eerste evaluaties van cameraprojecten de veiligheidseffecten ervan relativeren.

Tweemaal bracht het CBP in 2002 advies uit over het wetsvoorstel cameratoezicht op openbare plaatsen. Vanuit het oogpunt van rechtszekerheid is een wettelijk kader van belang. Het CBP kon zich goed verenigen met de toekenning van de bevoegdheid tot plaatsing van camera's aan de burgemeester op basis van een verordening van de raad. Een dergelijke toedeling komt overeen met de verantwoordelijkheid van de burgemeester voor de handhaving van de openbare orde.

Onder de reikwijdte van het cameratoezicht bleken ook de kerken en vergelijkbare plaatsen te vallen. Is het de bedoeling dat de overheid met het oog op de openbare orde camera's kan plaatsen in kerken, moskeeen en andere gebouwen bestemd voor de belijdenis van een levensovertuiging?

Elektronische overheid

De overheid brengt langzaam maar zeker steeds meer structuur aan in haar informatiehuishouding met het oog op een efficiënte en betrouwbare taakvervulling. Deze ontwikkeling brengt belangrijke kansen en bedreigingen met zich mee voor de bescherming van persoonsgegevens. In 2002 heeft het CBP een uitgewerkte visie neergelegd in de studie *Elektronische overheid en privacy: bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid*. De studie richt zich met name op de beleidsmakers, bespreekt privacy-ontwerpprincipes voor informatiesystemen en geeft een analyse van de speelruimte die de privacyregels bieden.

Vertrouwen is een essentiële voorwaarde voor een goed functionerende informatie-infrastructuur. Het CBP heeft daarom reserves ten aanzien van het pleidooi de burger 'de regie' over zijn eigen persoonsgegevens geven. De overheid moet inderdaad zorgen voor optimale transparantie, maar er zijn evidente grenzen aan informationele zelfbeschikking. In de WBP is bewust gekozen voor een systeem van *checks and balances* waarin toestemming en verzet slechts een corrigerende rol spelen. Belangrijker is dat de overheid ook zonder regie-aanwijzingen van de burger transparant en vertrouwenwekkend werkt.

Burgerservicenummer

Het CBP heeft vanuit zijn visie op de elektronische overheid ook een bijdrage geleverd aan het advies van de interdepartementale commissie Van Thijn, *Persoonsnummerbeleid in het kader van identiteitsmanagement*. Het CBP was vertegenwoordigd in de commissie. Het kabinet onderschreef het advies en

Resultaten 2002

IN HET VORIGE JAARVERSLAG IS AANGEKONDIGD DAT IN 2002 ZOU WORDEN GESTREEFD NAAR DE VOLGENDE RESULTATEN:

- **Elektronische overheid**
  In de studie *Elektronische overheid en privacy* heeft het CBP laten zien hoe de overheid door de inzet van ICT beter kan werken met behoud en versterking van privacywaarborgen. Deze visie heeft bijgedragen aan het overheidsbeleid met betrekking tot de stroomlijning van basisgegevens en het gebruik van persoonsnummers.

- **Informatietechnologie in de zorg**
  In de studie *Privacy bij ICT in de zorg* heeft het CBP aangegeven hoe privacybescherming beter kan worden verankerd in de gezondheidszorg. De inhoud van de studie is binnen de sector breed uitgedragen. Tijdige en adequate aandacht voor privacybescherming is een kritische succesfactor bij nieuwe ontwikkelingen op dit terrein.

- **Onderzoek en statistiek**
  In de notitie *Privacy bij wetenschappelijk onderzoek en statistiek* zijn de wettelijke regels voor het gebruik van persoonsgegevens op dit gebied verhelderd. De notitie bevat ook een kader voor de ontwikkeling van een gedragscode waarin die regels naar de praktijk kunnen worden vertaald. De Koninklijke Nederlandse Academie van Wetenschappen heeft hiertoe het initiatief genomen.

- **Werknemers**
  Een nieuwe versie van de studie *Goed werken in netwerken*, een nieuwe *Raamregeling voor het gebruik van e-mail en internet* en de brochure *Privacy: checklist voor de ondernemingsraad* hebben het belang van goede privacybescherming op het werk nadrukkelijk onder de aandacht gebracht. Ook is de basis gelegd voor een publicatie over de positie van zieke werknemers.

- **Handelsinformatie**
  Het is in 2002 nog niet mogelijk gebleken om binnen de branche overeenstemming te bereiken over duidelijke normen voor een rechtmatige verwerking van persoonsgegevens en waarborgen voor een juiste naleving daarvan. De behoefte aan normen en waarborgen is bij onderzoeken opnieuw gebleken. Het CBP heeft hierin aanleiding gevonden om met meer inzet op te treden.

- **Gebruik van telecommunicatie**
  Het CBP heeft een verkennend onderzoek verricht naar de verwerking van gegevens over het gebruik van telecommunicatie. De resultaten hebben ten grondslag gelegen aan een workshop die in september 2002 is georganiseerd samen met het Instituut voor Informatierecht (UvA) en mogelijk werd gemaakt mede door de OPTA. De uitkomst is neergelegd in de studie *Verkeersgegevens* die ook voor het CBP een basis zal vormen voor verdere activiteiten op dit gebied.

kondigde aan in 2003 een voorstel te zullen uitwerken voor een 'burgerservicenummer'.

De invoering van een burgerservicenummer dient de eenduidige identificatie van gegevens van burgers voor een doelmatiger en klantgerichter overheid. Het nummer maakt de koppeling van gegevens tussen overheden mogelijk en is daardoor ook belangrijk voor opsporing en bestrijding van (identiteits)fraude.

Het beoogde sectorale persoonsnummerbeheer is in lijn met de visie van het CBP op de elektronische overheid en de voorkeur voor sector- en ketennummers. De sectoren Justitie en Zorg zullen volgens het advies aparte sectornummers gebruiken. De rechtmatige verwerking van gegevens zal bevorderd worden door de vertrouwensfuncties, die onder meer bestaan uit Privacy-Enhancing Technologies, dus technische privacywaarborgen in de informatiesystemen zelf.

Dossiers van de sociale dienst

In de sfeer van de sociale zekerheid is diepgaande controle van individuen noodzakelijk. In februari 2002 werd een dossieronderzoek uitgevoerd bij drie sociale diensten. Onderzocht werd of de gegevens in de dossiers noodzakelijk waren voor de vaststelling van het recht op bijstand (noodzakelijkheidsvereiste). Verder is nagegaan van welke instanties de sociale diensten gegevens ontvingen en aan welke instanties zij gegevens verstrekten. Het CBP heeft een positieve indruk gekregen van de wijze waarop de drie sociale diensten met persoonsgegevens omgaan, maar overweegt wel over enige tijd een handhavingsonderzoek te doen bij sociale diensten.

- **Bijzondere politieregisters**
  In 2002 zijn verbeteringen zichtbaar geworden bij de politieregisters met 'criminele inlichtingen'. Zowel het beheer als het structurele toezicht op deze registers hebben bij de meeste korpsen meer aandacht gekregen. Ook is overeenstemming bereikt over een stroomlijning van de behandeling van verzoeken om inzage door betrokkenen. De resultaten zijn binnen de politie en het Openbaar Ministerie breed uitgedragen.

- **Openbaar register van WBP-meldingen**
  Op de CBP-website is een openbaar register van ontvangen meldingen voor iedereen toegankelijk geworden. Naast een verbeterde versie van het WBP-meldingenprogramma op diskette is nu ook een melding via internet mogelijk. Het aantal meldingen is in de loop van 2002 sterk toegenomen. De CBP-website bevat ook een openbaar register van functionarissen voor de gegevensbescherming.

- **Voorafgaand onderzoek**
  Het aantal voorafgaande onderzoeken naar verwerkingen met bijzondere risico's (artikelen 31-32 WBP) is sterk toegenomen. Een overzicht zal in de loop van 2003 op de CBP-website verschijnen. Voor een aantal veel voorkomende verwerkingen zijn in overleg met belanghebbenden inmiddels standaarden ontwikkeld (bijv. sociale recherche van de Gemeentelijke Sociale Diensten).

- **Handhavingsplan**
  In 2002 is een afdeling Interventie, bezwaar en beroep in het leven geroepen. De ontwikkeling van een handhavingsplan heeft inmiddels geleid tot een aantal instrumenten die het CBP in staat stellen om zijn nieuwe bevoegdheden effectief te gebruiken. Ook is een begin gemaakt met een systematische controle op de naleving van de meldingsplicht.

Jeugdzorg: intaketeams en informatie-uitwisseling

Het Bureau Jeugdzorg zal met de invoering van de nieuwe Wet op de jeugdzorg de hulpvraag van jeugdigen vertalen in een indicatie voor de gewenste zorg. Het inrichten van één 'balie' betekent dat de verschillende soorten zorg bij de Bureaus Jeugdzorg vertegenwoordigd zullen zijn: jeugdbescherming, jeugdhulpverlening en de jeugd Geestelijke Gezondheidszorg. Het doel is een multidisciplinaire diagnostiek.
De bij deze intake betrokken hulpverleners werken vaak voor een instelling in een van de vertegenwoordigde sectoren maar fungeren ook als medewerkers van het bureau. In een dergelijke dubbele functie ontstaat in de praktijk gemakkelijk het idee dat informatie over reeds bekende cliënten voor de intake onderling mag worden uitgewisseld.
Wanneer de hulpvrager al bekend is bij een van de 'intakers', heeft deze een flink dilemma. Als in het intaketeam de 'eigen' cliënt ter sprake komt, heeft hij enerzijds te maken met zijn beroepsgeheim, anderzijds met de verwachting, mogelijk ook de neiging, om informatie over de cliënt die al eerder is verkregen bij de intake te gebruiken. Een van de betrokken hulpverleners legde de situatie voor aan het CBP.
Het inrichten van een Bureau Jeugdzorg betekent niet dat persoonsgegevens onbeperkt uitgewisseld kunnen worden. Het beroepsgeheim geldt onverkort, ook in dergelijke dubbelfuncties. Bij het eerste contact met de hulpvrager zou bijvoorbeeld kunnen worden gevraagd naar eerdere ervaringen met jeugdzorg. Door gerichte samenstelling van het intaketeam kan het dilemma vermeden worden.
Bij het eerste contact moet ook toestemming worden gevraagd om eventueel informatie in te winnen bij een eerdere behandelaar. Ook doorverwijzing vanuit de instellingen naar het intaketeam kan alleen met inachtneming van het beroepsgeheim. Toestemming van de betrokkene voor het verstrekken van gegevens aan het intaketeam betekent niet dat daarmee ook toestemming is gegeven voor verdere verstrekkingen. Steeds zal moeten worden bezien of opnieuw toestemming nodig is of dat een andere grondslag verdere verstrekking rechtvaardigt.
Het Bureau Jeugdzorg zal de gegevens bij hulpvragers kunnen verzamelen die noodzakelijk zijn voor intake en indicatiestelling. Doorverstrekking van deze gegevens, voor zover noodzakelijk voor zorgtoewijzing en zorgverlening, is onder voorwaarden ook mogelijk. Een belangrijke voorwaarde is dat hulpvragers vooraf op de hoogte zijn gebracht van de gang van zaken. Degene aan wie de gegevens verstrekt worden, moet bovendien direct betrokken zijn bij de aan de betreffende jeugdige aan te bieden zorg ●

Een nieuwe bijstandswet

Eind 2002 heeft het CBP geadviseerd over het voorstel voor een nieuwe bijstandswet, inmiddels Wet werk en inkomen geheten. De nieuwe wet zal een groot aantal bestaande wettelijke regelingen vervangen. Door gemeenten een grotere bewegingsvrijheid te geven bij de invulling van de individuele rechten en plichten en bij het aanbieden van voorzieningen beoogt het kabinet de reintegratie van werkzoekenden te versnellen.ïntegratie van werkzoekenden te versnellen.

Het CBP had de Minister van Sociale Zaken en Werkgelegenheid al verscheidene malen verzocht om heldere regels te stellen voor de overdracht van persoonsgegevens bij reintegratie.Het moest constateren dat ook dit wets-ïntegratie. Het moest constater voorstel geen helderheid geeft over hoe gegevensverwerking bij reintegratie praktisch vorm dient te krijgen. Veel lijkt overgelaten te worden aan de gemeenten. Hierin schuilt het gevaar dat er verschillen tussen gemeenten optreden bij de uitvoering van de reintegratietaak.

Sociale recherche en fraudeteams

De strijd tegen fraude bij de sociale zekerheid stond in 2002 sterk in de belangstelling. Deze fraudebestrijding wordt uitgevoerd door allerlei organisaties. Het gaat om de (gemeentelijke) sociale recherches, de Regionale Interdisciplinaire Fraudeteams (RIF) en de Sociale Inlichtingen- en Opsporingsdienst (SIOD). Het CBP heeft in het kader van de melding van enkele informatieverwerkingen een voorafgaand onderzoek verricht ter beoordeling van de rechtmatigheid van de inrichting van de verwerking. Vergelijkbaar onderzoek werd gestart naar de rechercheactiviteiten van het Uitvoeringsinstituut Werknemersverzekeringen en de Sociale Verzekeringsbank.

Het CBP heeft onderzoek gedaan naar de procesbeschrijving voor heimelijke waarneming die door één van RIF's was opgesteld, en de daaruit voortvloeiende werkwijze beoordeeld. De naleving van de procesbeschrijving bood in beginsel voldoende waarborgen voor een rechtmatige verwerking van persoonsgegevens. Afgesproken werd dat de procesbeschrijving ook voor andere RIF's als leidraad kon dienen. Een dergelijke aanpak heeft het CBP ook gevolgd ten aanzien van de sociale recherches van de gemeenten.

Belangrijke winst van de gekozen benadering kan een brede, landelijke harmonisering zijn van de werkwijze bij heimelijke waarneming van de RIF's en van de (gemeentelijke) sociale recherches. Rechtszekerheid en het nalevingsniveau van de WBP worden hierdoor bevorderd terwijl de noodzakelijke melding eenvoudiger kan worden afgehandeld.

Zwarte lijsten

Ook het bedrijfsleven zocht in 2002 nadrukkelijk naar maatregelen tegen criminaliteit. Tegen de achtergrond van onvrede over wat politie en justitie voor bedrijven konden doen, groeide de behoefte om zelf paal en perk te stellen aan wangedrag en fraude van klanten of eigen personeelsleden. Zwarte lijsten worden gezien als deel van de oplossing. Het CBP heeft in 2002 onder meer nauwkeurig gekeken naar de zwarte lijst van de gezamenlijke financiële instellingen.

Dat bedrijven bij het voeren van zwarte lijsten een gerechtvaardigd belang kunnen hebben staat eigenlijk niet ter discussie. De vraag is vooral of het belang van het bedrijf opweegt tegen de individuele consequenties van plaatsing op een zwarte lijst. Als besloten wordt een zwarte lijst in te voeren, moet het bedrijf waarborgen treffen om een dergelijk systeem zorgvuldig te gebruiken. Zonder dergelijke waarborgen is een zwarte lijst verboden.

Waarschuwingslijsten als middel tegen frauderende werknemers kregen veel publiciteit. Het CBP heeft diverse lijsten beoordeeld. De gevolgen van plaatsing worden sterk bepaald door de reikwijdte van de zwarte lijst. Deze kan gelden voor noodzakelijke functies of voor alle werknemers, voor een bedrijf al dan niet met filialen, een concern of zelfs een hele bedrijfstak. De criteria voor plaatsing moeten strikter worden wanneer de reikwijdte van de lijst toeneemt.

Goed werken in netwerken

Goede motivering en inrichting van controle kan voorkomen dat noodzakelijke fraudebestrijding de relatie met werknemers onnodig belast. Een goede afweging van belangen is hierbij de sleutel. Een verantwoorde controle op (privé)gebruik van e-mail en internet op het werk vereist een privacytoets en goed overleg met de werknemers of de instemming van de ondernemingsraad. Om een goede regeling binnen bedrijven te bevorderen publiceerde het CBP in 2002 een geactualiseerde versie van *Goed werken in netwerken*, een nieuwe *Raamregeling voor het gebruik van e-mail en internet* en de brochure *Privacy: checklist voor de ondernemingsraad*. Voor deze handreikingen bleek in 2002 grote belangstelling.

Privacy bij ICT in de zorg

In 2002 publiceerde het CBP ook de studie *Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg*. Doel van de studie is een overzicht van de privacyaspecten van de toepassing van ICT in de zorg. De vele beleidsvoornemens,

experimenten en trends bij ICT in de zorg zullen leiden tot een elektronische identiteitsinfrastructuur, een elektronische informatie-infrastructuur en veranderingen in de organisatie en de financiering van de zorg. Bij de huidige ICT-toepassingen is privacy onvoldoende als ontwerpcriterium meegenomen. Tijdige én adequate aandacht voor privacybescherming in de zorg is echter een kritische succesfactor.

Bij de stelselherziening gaat het vooral om meer concurrentie tussen aanbieders van zorg en tussen zorgverzekeraars. Vergoeding van de zorg moet worden gerelateerd aan de werkelijk gemaakte kosten. Als onderdeel van de stelselwijziging zal de zogeheten Diagnose-Behandeling Combinatie(DBC)-systematiek worden ingevoerd. Bij de uitwerking van het DBC-concept dient de overheid zich rekenschap te geven van de verschillende rollen van de zorgverzekeraar en de andere partijen in de gezondheidszorg. Gedetailleerde behandelingsgegevens mogen niet zomaar worden verstrekt. De privacywetgeving en het medisch beroepsgeheim stellen dwingend grenzen aan de verwerking van (bijzondere) persoonsgegevens.

Handelsinformatiebureaus

Een ronduit onbevredigende situatie bestaat in de sector van de handelsinformatiebureaus. In 2002 heeft het CBP andermaal bij een bureau een diepgaand onderzoek moeten uitvoeren; elders in dit jaarverslag (p. 22) wordt een impressie gegeven van wat werd aangetroffen. Kennelijk is meer nodig dan incidenteel toezicht om de handelsinformatiebranche zich te laten voegen naar het wettelijke kader voor de verwerking van persoonsgegevens.

Bedrijven hebben een evident belang bij goede creditscoring en verhaalsinformatie. Dat dient echter wel in balans te worden gebracht met het algemene belang dat is gemoeid met een betrouwbaar en integer functioneren van overheden en bedrijven in hun omgang met persoonsgegevens. Een oplossing dient wellicht gezocht te worden in nadere regelgeving voor het verkrijgen van persoonsgegevens voor creditscoring en incasso.

Stadionverbod bij Feijenoord

Misdragingen van supporters, gewelddadigheden door een harde kern van hooligans, voetbalclubs zien zich al jaren genoodzaakt hier tegen op te treden. Een van de middelen die ingezet worden, is het stadionverbod. Een stadionverbod kan wel, maar niet zomaar.
Een stadionverbod kan worden opgelegd door de rechter of door een stadion c.q. voetbalvereniging, een zogenaamd civiel stadionverbod. Een door de rechter opgelegd stadionverbod geldt landelijk. Een dergelijk verbod naar aanleiding van onrechtmatig of hinderlijk gedrag valt onder de bepalingen in de Wet bescherming persoonsgegevens voor strafrechtelijke gegevens. Dat betekent dat het in principe verboden zou zijn deze gegevens te verwerken ten behoeve van derden, in dit geval dus andere clubs die het verbod moeten handhaven. Deze clubs moeten er immers van weten en de gegevens ook verwerken in hun 'zwarte lijst'.

Telecommunicatie

De telecommunicatiesector wordt geconfronteerd met uitgebreide regelgeving op grond van Europese richtlijnen, nationale wetten en jurisprudentie. Het CBP signaleerde onzekerheid in de sector bij het toepassen van de privacynormen. Het CBP zal zich in 2003 inspannen de sector op concrete punten te informeren over de geldende normen. Samen met de OPTA startte het CBP een onderzoek naar de verkoop door KPN van adresgegevens behorende bij zogenaamde 'geheime' nummers voor marketingdoeleinden. Het CBP streeft er naar de samenwerking met de OPTA op het gebied van het toezicht verder uit te werken.

De voornaamste kwestie die in 2002 vanuit privacyoptiek in de sector speelde, was die van het bewaren en gebruiken van verkeersgegevens. Telecomaanbieders verzamelen enorme hoeveelheden gegevens over de telecommunicatie van individuen (vaste en mobiele telefonie en internet), zij bewaren deze gegevens ook na afloop van de communicatie en voor hen is het verdere gebruik van deze gegevens voor allerlei innovatieve diensten van groot commercieel belang. Marketing op basis van telecommunicatiegegevens is van strategische waarde. In 2002 heeft het CBP een verkennende studie gedaan naar het afrekenen en verrekenen van telecommunicatiediensten als oriëntatie op het feitelijke gebruik van verkeersgegevens.

Opsporing en verkeersgegevens

In samenwerking met het CBP organiseerde het Instituut voor Informatierecht van de Universiteit van Amsterdam in september 2002 een seminar over de technische, publiekrechtelijke en strafvorderlijke aspecten van verkeersgegevens. Het CBP pleitte ook bij die gelegenheid voor grote terughoudendheid bij de opslag van verkeersgegevens. Verkeersgegevens geven in de context zeer veel informatie. Het grondrecht op vertrouwelijke communicatie is hierdoor in het geding.

Het verbod op het verwerken van strafrechtelijke gegevens ten behoeve van derden is echter niet van toepassing als onder meer 1) de verwerking plaats vindt door verantwoordelijken met een vergunning voor particuliere beveiligingsorganisaties en recherchebureaus of 2) indien waarborgen zijn getroffen en bij de toezichthouder een voorafgaand onderzoek is aangevraagd.
De Stichting Feijenoord en het Stadion Feijenoord NV zijn samen verantwoordelijk voor het verwerken van dergelijke gegevens. Aangezien alleen het Stadion Feijenoord NV beschikt over de vereiste vergunning is in dit geval het verbod niet van toepassing wanneer voldaan is aan de tweede voorwaarde. Er moest dus bij het CBP een voorafgaand onderzoek worden aangevraagd bij de melding van de zwarte lijst en er moesten passende en specifieke waarborgen zijn getroffen.

Deze waarborgen bleken bij het voorafgaand onderzoek inderdaad aanwezig. Er zijn richtlijnen voor het opleggen van een stadionverbod met heldere criteria om willekeur te voorkomen. Stadionverboden worden opgelegd na overtreding van het toegangsreglement van het stadion. De toegangsvoorwaarden staan op het kaartje vermeld en worden aan het begin van het seizoen aan de kaarthouders toegezonden. Rondom het stadion hangen bij iedere ingang borden met voldoende informatie. Hierdoor is het voor de stadionbezoekers duidelijk wat de spelregels zijn om een stadionverbod te voorkomen. Daarnaast zijn er mogelijkheden voor inzage, correctie en aanvulling van de gegevens voor supporters die op de zwarte lijst komen.
Op grond van deze bevindingen achtte het CBP de door Feijenoord gemelde gegevensverwerking voor het opleggen van stadionverboden rechtmatig ●

Doelen 2003

In 2003 zullen met name de volgende resultaten worden nagestreefd:

- **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 zal in overleg met de betrokken departementen de randvoorwaarden ontwikkelen zodat op een adequate wijze invulling gegeven kan worden aan deze verplichting.

- **Functionarissen gegevensbescherming**
  Op grond van de artikelen 62-64 WBP zijn inmiddels meer dan honderd functionarissen voor de gegevensbescherming bij het CBP aangemeld. Het contact met dit groeiend netwerk van interne toezichthouders zal binnen het CBP zodanig worden geborgd, dat zich in de praktijk een goed samenspel tussen functionarissen en het CBP kan ontwikkelen.

- **Cameratoezicht**
  Het aantal gemeenten met cameratoezicht op openbare plaatsen is de afgelopen tijd aanzienlijk toegenomen. Het CBP zal een onderzoek uitvoeren naar de wijze waarop dit camera-toezicht in de praktijk functioneert en hoe met de privacy-aspecten daarvan in verschillende gemeenten wordt omgegaan.

- **Zieke werknemer**
  Door veranderingen in de sociale zekerheid en de samenleving is de positie van werknemers vóór, tijdens en na afloop van ziekte meer onder druk gekomen. Het CBP zal een studie publiceren waarin de privacyaspecten van deze positie centraal zullen staan en waarin de relaties met andere relevante ontwikkelingen op dit terrein zullen worden belicht.

- **Politieregisters**
  In het verlengde van eerdere activiteiten van het CBP met betrekking tot de registers van de Criminele Inlichtingen-eenheden (CIE's), zal een aantal van deze eenheden aan een nadere toets worden onderworpen. Daarbij zal mede gebruik worden gemaakt van de uitkomsten van interne evaluaties van de CIE's.

- **Telecommunicatie**
  Bij het verlenen van diensten op het gebied van de tele-communicatie doen zich in de praktijk verschillende privacy-vragen voor. In samenwerking met de OPTA zal het CBP voorlichtingsmateriaal ontwikkelen om meer duidelijkheid te verschaffen. Het CBP zal ook nadere aandacht besteden aan meldingsplicht en voorafgaande onderzoeken binnen de telecomsector.

- **Certificering**
  Op basis van de uitkomsten van het eerdere project Auditaanpak is de grondslag gelegd voor een systeem van privacycertificering. In samenwerking met aspirant-accreditatieinstellingen zal het CBP dit systeem nader ontwikkelen en gereed maken voor invoering. Doel hiervan is de naleving van privacywetgeving via zelfregulering verder te bevorderen.

- **Internetsite**
  Een goed ingerichte website is een centraal onderdeel van de voorlichtingsstrategie van het CBP. De toegankelijkheid van de CBP-website zal worden verbeterd, onder meer door de intro-ductie van themadossiers en de ontwikkeling van een aparte sectie voor vragen van betrokkenen. Op deze website zal ook het beleid van het CBP met betrekking tot de verschillende zaaksoorten worden bekendgemaakt.

- **Meldingsplicht**
  De verplichting om verwerkingen van persoonsgegevens bij het CBP te melden draagt bij aan transparantie en controleer-baarheid. De handhaving van deze verplichting zal door inzet van systematische controle ter hand worden genomen. In het verlengde daarvan zal gebruik worden gemaakt van de bevoegdheid tot het opleggen van een bestuurlijke boete bij overtredingen.

- **Formatieplan**
  Om een goede uitvoering van nieuwe taken op het terrein van toezicht en handhaving te kunnen verzekeren, zullen de organisatie en formatie van het CBP worden aangepast. In de loop van het jaar zal een nieuw formatieplan met nieuwe of aangepaste functieprofielen worden vastgesteld.

Wie wat bewaart

In de telecommunicatiesector wordt van elk en ieder gesprek een hele reeks technische gegevens – onder andere de nummers van de gelegde verbinding, duur, datum en tijdstip - vastgelegd. Dat is alleen al noodzakelijk voor het sturen van een rekening aan de klanten en voor de verrekening tussen de telecomaanbieders onderling. De verkeersgegevens mogen vervolgens een beperkte tijd bewaard worden voor het geval er discussie over een rekening ontstaat. Dit is bepaald in de Telecommunicatiewet. Deze geeft verder nog ruimte voor het verwerken van deze verkeersgegevens voor de marketing van eigen telecommunicatiediensten op voorwaarde dat de abonnee daarmee heeft ingestemd.
Een van de vele in Nederland actieve telecomaanbieders gaf in de melding van zijn verwerkingen van persoonsgegevens aan dat de verkeersgegevens maar liefst drie jaar bewaard bleven. Een dergelijke termijn is langer dan nodig voor rekeningdoeleinden en voldoet niet aan de hiervoor geldende wettelijke norm. Als voornaamste doel van het zo lang bewaren werd echter genoemd het gebruik van de gegevens voor marketing en verkoop van de eigen diensten. In de algemene voorwaarden bij de overeenkomsten met de abonnees lag dat al vast zodat de klant hiermee akkoord was gegaan.
Het CBP was van oordeel dat dit niet kon gelden als de vereiste vrije en gerichte toestemming van de klant. Een abonnee behoort een reële mogelijkheid te worden geboden zich over het specifieke gebruik van verkeersgegevens voor marketingdoeleinden uit te spreken. Bovendien werd de klant op geen enkele manier geïnformeerd over het bewaren van de gegevens en het doel daarvan. Niet duidelijk was dat de gegevens in de praktijk drie jaar bewaard bleven of dat marketingprofielen werden gemaakt.
In het kader van het onderzoek naar de melding, waaruit ook de heimelijke vastlegging van alle telefonische contacten van klanten met de helpdesk bleek, kwam het CBP tot de conclusie dat de gemelde gegevensverwerking een verwerking was zoals bedoeld in artikel 31, eerste lid, sub b WBP: gegevens vastleggen op grond van eigen waarneming zonder de betrokkene daarvan op de hoogte te stellen.
Het advies was de verwerking, die in de gemelde vorm onrechtmatig was, anders in te richten en opnieuw te melden ●

In het klimaat van na *September 11* ontstond een sterke politieke beweging om deze data voor het doel van opsporing en strafvordering zeer lang te doen bewaren. Op Europees niveau werd in 2002 door regeringen gesproken over een systematische bewaarplicht voor de verkeersgegevens van alle telefoongesprekken, faxverkeer, e-mails en overig gebruik van internet. Deze zouden bewaard moeten blijven voor politie, justitie en veiligheidsdiensten. Dit is een ernstige bedreiging van de bescherming van de persoonlijke levenssfeer.

Op 3 september 2002 liet het CBP de Minister van Justitie weten dat het een algemene bewaarplicht voor verkeersgegevens van een jaar of meer oneven-redig en in geen geval toelaatbaar achtte. Op 11 september 2002 gaven de Europese privacytoezichthouders, bijeen in Cardiff, een verklaring van dezelfde strekking uit. Europese regelgeving maakt het bewaren van verkeersgegevens voor het doel van de rechtshandhaving alleen mogelijk voor een beperkte periode en alleen voor zover noodzakelijk, passend en proportioneel in een democratische samenleving.

Privacy-Enhancing Technologies

De afgelopen jaren heeft het CBP veel geinvesteerd in de ontwikkeling en het uitdragen van het concept van de Privacy-Enhancing Technologies (PET). Het door het CBP georganiseerde PET-symposium in mei 2002 liet zien dat deze aanpak zich in de praktijk heeft bewezen en *proven technology* is geworden. PET heeft ook een belangrijke plaats gekregen in het toekomstige persoonsnummerbeleid van de overheid.

Het doel van het symposium was beleidsmakers van overheid en private sector de praktische bruikbaarheid van het PET-concept te laten zien. Door privacyregels mee te nemen in het ontwerp van het informatiesysteem kan immers een rechtmatige verwerking van persoonsgegevens (deels) gegarandeerd worden: *privacy by design*. Vanuit een oogpunt van privacybescherming is het beter dat iets niet kan, dan dat het alleen maar verboden is. Uit de zorgsector werden drie werkende informatiesystemen gepresenteerd; in het internationale gedeelte werden de ervaringen met het PET-concept in Canada en Duitsland belicht.

Certificering

De WBP-assurance producten *WBP Zelfevaluatie* en *Raamwerk Privacy Audit* vonden in 2001 en 2002 gretig aftrek evenals de CBP-studie *Beveiliging van persoonsgegevens (2001)*. Het CBP heeft in 2002 minder aandacht gegeven aan voorlichting over deze auditaanpak en heeft zijn inspanningen vooral gericht op privacycertificering. Daarbij beoogt het CBP commerciële audit-organisaties een kader te bieden voor het verlenen van privacycertificaten. In nauw overleg met de beroepsorganisaties die kunnen optreden als accreditatie-instelling, is het schema opgesteld op basis waarvan auditors geaccrediteerd kunnen worden als privacy auditor. Bij het opstellen van de certificeringseisen speelt het *Raamwerk Privacy Audit* een sleutelrol. De eerste opzet van een certificatieschema is voorbereid en enkele brancheorganisaties zijn bereid als accreditatie-instellingen op te treden voor het erkennen van auditors die de bevoegdheid krijgen om erkende privacycertificaten voor specifieke verwerkingen af te geven.

Gedragscodes

In 2002 is de Gedragscode van de Nederlandse Vereniging van de Research-georiënteerde Farmaceutische Industrie (Nefarma) als eerste gedragscode onder de WBP voorzien van een goedkeurende verklaring. Een gedragscode dient een uitwerking te geven van de WBP en andere wettelijke bepalingen voor de verwerking van persoonsgegevens specifiek voor de sector. In 2002 is ook uitvoerig overleg gevoerd over een gedragscode met de banken en verzekeraars. In januari 2003 kon deze belangrijke Gedragscode Verwerking Persoonsgegevens Financiële Instellingen worden goedgekeurd.

Ook de Nederlandse Vereniging van Handelsinformatiebureaus heeft in 2002 overleg gevoerd met het CBP over een conceptgedragscode maar resultaat werd helaas nog niet bereikt. Dit klemt te meer gezien de situatie in de sector. Met de branchevereniging van particuliere beveiligings- en recherchebureaus – een onvoldoende gereglementeerde en sterk groeiende sector – werd gewerkt aan een gedragscode evenals met de brancheorganisatie voor reintegratiebedrijven (Borea) en de Koninklijke Beroepsvereniging van Gerechtsdeurwaarders. De verwachting is dat deze gedragscodes in 2003 zullen worden goedgekeurd.

Wetgevingsadvisering

In lijn met het viersporenbeleid stelt het CBP zich pro-actief op als adviseur en onderhoudt het actief contact met de overheid en andere organisaties. In het najaar van 2002 is het CBP gesprekken met de ministeries gestart om de wettelijke adviesfunctie van het CBP onder de aandacht te brengen. Er bleek bij de ministeries niet alleen onbekendheid met de nieuwe regelgeving maar ook onzekerheid over de reikwijdte van de verplichting. Het CBP streeft ernaar de adviesverplichting deel uit te laten maken van de wetgevingsprocedure. Dit moet leiden tot een meer structurele invulling van de adviestaak van het CBP en tot een intensivering van de werkzaamheden op dit terrein.

Sleutelen aan modelcontracten

Multinationals sturen heel wat persoonsgegevens rond tussen Europa en de rest van de wereld. Voor doorgifte van persoonsgegevens aan landen buiten Europa zonder passende privacybescherming is veelal een vergunning nodig. Het CBP beoordeelt de vergunningaanvraag en adviseert de minister over het verlenen ervan. Daarbij kunnen bedrijven een doorgifte regelen op basis van modelcontracten goedgekeurd door de Europese Commissie. Wanneer een modelcontract ongewijzigd wordt gebruikt, wordt in principe de vergunning verleend.

Het CBP ontving een vergunningaanvraag van een multinational waarvan de Nederlandse vestiging financiële diensten verleent. De Nederlandse vestiging wilde gegevens doorgeven aan een zusterorganisatie in de VS, die op zou treden als 'bewerker'. Een bewerker verwerkt persoonsgegevens op instructie en onder verantwoordelijkheid van de opdrachtgever. Het bedrijf had het Europese modelcontract voor doorgifte aan een bewerker gebruikt en daarbij gewijzigd.

Het contract voorzag ook in overdracht van taken en onderaanbesteding door de Amerikaanse bewerker aan anderen. Dat betekent dus een verdere doorgifte van persoonsgegevens waarvoor de Nederlandse vestiging verantwoordelijk blijft. Ook deze derde partijen dienden dus gebonden te worden aan het contract met de verantwoordelijke. De mogelijkheid van de Nederlandse verantwoordelijke om de verwerking van de Amerikaanse bewerker te controleren was ingeperkt. Een audit zou alleen mogelijk zijn als er sprake zou zijn van (onder meer) een risico van ernstig nadeel voor de betrokkene. De mogelijkheid om de bewerker te controleren is echter een belangrijke garantie voor een adequate bescherming. Op basis van het modelcontract kan een betrokkene ook de bewerker voor geleden schade via de Nederlandse rechter aansprakelijk stellen als de gegevensexporteur niet meer aansprakelijk kan worden gesteld. Deze bepaling biedt de betrokkene dus een ruimere mogelijkheid zijn recht te halen en was niet opgenomen in het contract. De bepaling die stelt dat na vergunningverlening het contract niet kan worden gewijzigd, was door de aanvrager geclausuleerd: dit was toegestaan tenzij dit negatieve gevolgen zou hebben voor de bescherming van persoonsgegevens. De ratio van de contractuele waarborgen is echter het garanderen van adequate privacybescherming aan de betrokkenen. Afspraken in het contract die hiervoor bepalend zijn, kunnen dus niet worden gewijzigd nadat de vergunning is verleend. De aanvrager volgde de voorstellen door het doorgiftecontract op deze punten aan te passen. Het CBP bracht daarop een positief advies uit aan de Minister van Justitie, die vervolgens de vergunning voor doorgifte verleende ●