2001 in vogelvlucht

De digitale revolutie beïnvloedt meer dan wat ook de manier waarop de samenleving met informatie en dus ook met persoonsgegevens omgaat. Burgers en consumenten kijken gretig uit naar de voordelen van digitale dienstverlening. Zij houden echter ook hun aarzelingen over de veiligheid en vertrouwelijkheid van de online diensten en relaties. Marktpartijen en overheden - in de vastberaden wens om commerciële of politieke doelstellingen te verwezenlijken - zien privacywaarborgen nog te vaak als obstakels. Tegelijkertijd onderschatten zij de speelruimte die gecreëerd wordt door 'privacy' van begin af mee te nemen in het ontwerp van informatiesystemen en -processen.

Privacy is een succesfactor. Of het nu gaat om het elektronische overheidsloket, controle op e-mailgebruik van werknemers, opsporingsbevoegdheden voor de politie, uitwisseling van medische gegevens voor de reïntegratie van werknemers, de doorgifte van klantgegevens naar landen buiten Europa of de verkoop van adresgegevens voor direct marketing: een rechtmatige, integere omgang met persoonsgegevens is een voorwaarde voor commercieel en bestuurlijk succes. Zonder waarborgen voor de privacy zal het nodige vertrouwen bij burger en consument ontbreken.

Het College bescherming persoonsgegevens (CBP) heeft in 2001 vanuit deze gedachte de studie *Klant te koop, privacyregels voor adressenhandel* aangeboden op de jaarlijkse Direct Marketing-dagen aan de voorzitter van de brancheorganisatie, de DMSA. Het CBP wilde hiermee een einde maken aan de onzekerheid in de branche en duidelijkheid scheppen over de mogelijkheden voor adressenhandel binnen het kader van de wet.

Ook de commerciële belangen bij een soepel én rechtmatig gegevensverkeer met landen buiten de Europese Unie zijn gebaat bij duidelijkheid over de privacyvoorwaarden die gesteld worden aan de doorgifte van persoonsgegevens. Het CBP heeft daarom in 2001 het *Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act* gepubliceerd waarin deze problematiek stapsgewijs wordt uiteengezet. Voor de verantwoordelijke bedrijven en instellingen is hiermee in principe ook de rol van het CBP in het vergunningtraject transparant geworden.

Privacy en informatie- en communicatietechnologie

Het CBP investeerde ook in 2001 in onderzoek naar de bedreigingen en kansen die informatie- en communicatietechnologie scheppen voor de bescherming van de persoonlijke levenssfeer. De Registratiekamer publiceerde *Beveiliging van persoonsgegevens*, dat een kader biedt voor de implementatie van de Wet bescherming persoonsgegevens bij informatiesystemen. In 2001 werden ook de in samenwerking met overheid en bedrijfsleven ontwikkelde privacyauditinstrumenten voor de beoordeling en controle van informatiesystemen breed gepresenteerd.

Daarbij wees het CBP nadrukkelijk op de kansen van privacy bevorderende technologie. Deze technologie voorkomt de onnodige verwerking van persoonsgegevens in informatiesystemen, een vorm van *privacy by design*. Ronduit futuristisch is op dit gebied het Europese PISA-project waaraan het CBP in 2001 deelnam. De ambitie van het project Privacy Incorporated Software Agents is het ontwikkelen van ontwerpspecificaties voor autonome software agents die de 'eigenaren' in staat zullen stellen allerlei elektronische transacties te (laten) verrichten met behoud van zeggenschap over hun persoonsgegevens.

In de nabije toekomst kan Nederland een grootschalige invoering verwachten van zogenaamde *trusted third parties* (TTP's), zowel publiek als privaat. TTP's zullen een sleutelrol spelen door het uitgeven van digitale identiteitscertificaten. De Registratiekamer bracht daarom in 2001 het rapport *Sleutels van vertrouwen* uit, de eerste uitwerking van de implicaties van de Europese privacyrichtlijn en de Nederlandse Wet bescherming persoonsgegevens voor de TTP-sector.

Elektronische overheid

De mate van zorgvuldigheid waarmee overheid en instellingen persoonsgegevens uitwisselen, heeft de Registratiekamer soms grote zorgen gebaard. Vooral waar instellingen in samenwerkingsverbanden persoonsgegevens uitwisselen, is niet altijd duidelijk wie voor welke verwerking van persoonsgegevens verantwoordelijk is of zelfs maar kan zijn. In dergelijke situaties kan efficiënter gegevensverkeer ten nadele van het individu uitpakken of ronduit in strijd zijn met de wet. Deze samenwerking en uitwisseling van gegevens tussen overheidsinstellingen zal in de nabije toekomst uitgroeien tot een vaste informatie-infrastructuur. Het CBP heeft daarom in 2001 de privacyaspecten van de overheidsplannen op het gebied van de 'elektronische overheid' onderzocht. In 2002 zal het CBP zijn visie op elektronische overheid en privacy publiceren.

Politieregisters

De registratie van burgers bij politie en justitie en de wijze waarop informatie over hen wordt vergaard, kan ingrijpende gevolgen hebben voor hun privacy. Het CBP en de Registratiekamer hebben hiervoor een bijzondere belangstelling. Vooral de registers van de Criminele Inlichtingeneenheden (CIE) vormen een grote bedreiging voor de privacy.

Verkoop van gegevens na faillissement

Bestanden met persoonsgegevens zijn geld waard. Na een faillissement wordt daarom vaak overwogen het bestand te verkopen. Dit gebeurt zowel met klantenbestanden als met kandidatenbestanden of personeelsbestanden. In 2001 speelde het geval van een bureau voor werving en selectie dat na faillissement zijn kandidatenbestand uit privacyoverwegingen grotendeels vernietigd had.

De curator stelde dat het klantenbestand een financiële waarde had en had daarom om overgave van de administratie gevraagd. De curator deed vervolgens aangifte bij de politie van het vermoedelijk plegen van bedrieglijke bankbreuk. De vraag was nu of het kandidatenbestand aan een derde verstrekt/verkocht had mogen worden. Er was geen wettelijk voorschrift om dit te doen en het zou ook niet gebeurd zijn met de toestemming van de geregistreerden. De curator zou het kandidatenbestand dus alleen aan een ander bureau hebben mogen verkopen als de verkoop zou zijn voortgevloeid uit het doel van de registratie.
Een werving- en selectiebureau heeft als doel het bemiddelen voor de kandidaten bij het vinden van geschikt werk. Dat is dus ook het doel voor het registreren van de

Resultaten 2001

IN HET VORIGE JAARVERSLAG IS AANGEKONDIGD DAT IN 2001 ZOU WORDEN GEMIKT OP DE VOLGENDE RESULTATEN:

• Voorlichtingscampagne

Rond de invoering van de Wet bescherming persoonsgegevens is in samenwerking met de ministeries van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties een voorlichtingscampagne gehouden. De Registratiekamer verzorgde de voorlichting aan koepel- en brancheorganisaties. Daarbij kon op de specifieke behoefte van elke branche worden ingespeeld.

• Internetsite & informatiemateriaal

De internetsite van het CBP (www.cbpweb.nl) is opnieuw ingericht en toegankelijker gemaakt. Verdere verbeteringen zijn in 2002 te verwachten. Het informatiemateriaal is integraal herzien en uitgebreid. Alle publicaties zijn op de website gratis beschikbaar.

• Zelfregulering

Er is een brochure uitgebracht over de mogelijkheid om een 'functionaris voor de gegevensbescherming' aan te stellen (artikel 62 e.v. WBP). Aanmeldingen voor de eerste tientallen functionarissen zijn ontvangen en verwerkt. Een toetsingskader is ontwikkeld voor organisaties die overwegen om een gedragscode te gaan opstellen (artikel 25 WBP). Een brochure daarover is in productie.

• Beveiliging & PET

Het rapport *Beveiliging van persoonsgegevens* geeft aan hoe invulling kan worden gegeven aan de verplichting om persoonsgegevens op een passende wijze te beveiligen (artikel 13 WBP). In een aparte brochure is ingegaan op de inzet van "Privacy-Enhancing Technologies' (PET). Een symposium over dit onderwerp is in voorbereiding genomen.

• Auditaanpak

Samen met koepelorganisaties en marktpartijen is een methode ontwikkeld om de kwaliteit van gegevensbescherming binnen organisaties systematisch te beoordelen. De producten van dit project *(Quickscan, WBP Zelfevaluatie en Raamwerk Privacy Audit)* zijn op de CBP-website voor ieder toegankelijk en worden in de praktijk toegepast. In een vervolgproject worden de mogelijkheden van certificering onderzocht.

• Meldingen

Tijdig vóór de invoering van de nieuwe wet is een WBP-meldingsprogramma ontwikkeld waarmee een WBP-melding kan worden opgesteld en ingezonden op een diskette. Het programma voorziet in een handreiking om te bepalen of er sprake is van een vrijstelling. De handreiking is raadpleegbaar op de CBP-website. Voor de melding zijn ook nieuwe formulieren met toelichting ontwikkeld.

persoonsgegevens van de kandidaten. Het doel van de registratie moet dus in de omstandigheden van het faillissement met zich meebrengen dat de gegevens worden doorverkocht.
Aannemelijk was echter wel dat de behoefte tot bemiddeling bij de ingeschrevenen ook na de faillietverklaring van het bureau nog bestond. Hoewel het doel van de registratie niet de verstrekking aan een nieuw bureau was, kan een dergelijke verstrekking daarom wel voortvloeien uit het oorspronkelijke doel. Dit betekent dat de verkoop van het kandidatenbestand aan een nieuw bureau rechtmatig had kunnen zijn.
Voor de beoordeling van de rechtmatigheid van de verkoop speelt echter ook een grote rol of de privacybelangen van de geregistreerden voldoende in acht zouden zijn genomen. Een voorwaarde is dat de kandidaten goed geïnformeerd zouden worden over de op handen zijnde verkoop en de mogelijkheid zouden krijgen hier bezwaar tegen te maken. Ook de aard van de gegevens en mogelijke gevolgen voor de betrokkenen kan er nog toe doen ●

• Handhaving

De werkprocessen voor het opleggen van bestuurlijke boete of last onder dwangsom, dan wel het toepassen van bestuursdwang, zijn in concept ontwikkeld en worden inmiddels ingevoerd. De uitgangspunten en beleidsregels voor het gebruik van deze bevoegdheden zullen in de loop van 2002 worden gepubliceerd.

• Werkprocessen

De werkwijzen en procedures voor de uitoefening van de overige taken en bevoegdheden zijn ontwikkeld en worden in fasen ingevoerd. De uitgangspunten en beleidsregels voor deze taken en bevoegdheden zullen in de loop van 2002 worden gepubliceerd.

• Derde landen

Een beleidsnota over gegevensverkeer met derde landen (artikel 76-77 WBP) staat op de CBP-website. Een brochure en informatieblad over hetzelfde onderwerp zijn daar ook beschikbaar. Gedrukte versies in het Nederlands en het Engels zijn in voorbereiding.

• Bestuur en organisatie

Een bestuursreglement is ontwikkeld en inmiddels goedgekeurd door de Minister van Justitie. Ook is een organisatie- en formatieplan vastgesteld, dat de basis vormt voor de invoering van competentiemanagement.

Het toezicht op en de kwaliteit van de registratie bleek in 2001 echter nog steeds beneden de maat. Wel constateerde het CBP zo langzamerhand een serieuze bereidheid bij politie en justitie om hier verbetering in te brengen. Inmiddels is in 2002 een circulaire van de minister van Binnenlandse Zaken en Koninkrijksrelaties in werking getreden waarin toezicht door middel van (externe) audits wordt voorgeschreven.

Opsporingsbevoegdheden

Bedrijven en instellingen kregen allerlei verzoeken en vorderingen van politie en justitie om inzage en afgifte van persoonsgegevens (van bijvoorbeeld klanten) uit computerbestanden. Deze vorderingen waren echter veelal onrechtmatig. Bedrijven kwamen hierdoor in een lastige positie. Naar aanleiding van de klachten heeft de Registratiekamer de minister van Justitie schriftelijk om een standpunt in deze kwestie verzocht. Inmiddels heeft de minister zich uitgesproken tegen een dergelijke wijze van informatie-inwinning.

De Commissie Strafvorderlijke gegevensverga-ring (Commissie Mevis) heeft in 2001 de kwestie van de politiebevoegdheden onderzocht. Zij stelde voor politie en justitie vergaande bevoegdheden te geven tot het vorderen van inlichtingen bij bedrijven en overheidsinstellingen. Het CBP daarentegen achtte een duidelijke wettelijke regeling nodig die alle belanghebbenden meer rechtszekerheid biedt. Een bedrijf of overheidsinstelling is geen verlengstuk van justitie of politie voor de opsporing.

De opsporingsinstanties zullen zorgvuldiger met informatie om moeten gaan. Volgens de voorstellen zal voortaan van grote groepen onverdachte personen informatie beschikbaar komen: een uitbreiding van bevoegdheden terwijl de huidige spelregels in de praktijk al niet voldoende bleken te worden nageleefd.

Vertrouwelijke communicatie

In het Wetsvoorstel vorderen gegevens telecommunicatie werd aan de gegevens over het telecommunicatieverkeer zelf categorisch de bijzondere bescherming van het grondrecht op vertrouwelijke communicatie onthouden. Het CBP meende en meent dat grote terughoudendheid geboden is bij het verplichten van de telecommunicatiesector tot het bewaren van gegevens in het algemeen. Het kabinetsvoorstel voor een nieuw artikel 13 Grondwet op basis van het eindrapport van de Commissie Grondrechten in het digitale tijdperk,

schoot echter in hoge mate te kort. Het grondrecht dient niet beperkt te worden tot de inhoud van het berichtenverkeer, maar moet zich ook uitstrekken tot de gegevens over het telecommunicatieverkeer zelf, de verkeersgegevens.

Controle van de werknemer

De werknemer ziet zijn werkplek meer en meer geautomatiseerd. Dat betekent ook dat hij wordt omringd door systemen die geschikt zijn als personeelsvolgsysteem: het digitale toegangspasje, de beveiligingscamera, GSM, RSI-programma's en andere software. De controle op het gebruik van e-mail en internet stond in 2001 maatschappelijk volop in de belangstelling. Het CBP heeft daarbij steeds duidelijk gemaakt dat de regelingen voor de controle op het werk maatwerk dienden te zijn en in bedrijven zelf tot stand dienden te komen. Het CBP heeft daarvoor ook hulpmiddelen aangeboden, die in 2002 opnieuw zullen worden uitgebracht; verder stelt het CBP zich hier op in tweede lijn.

De zieke werknemer

Het CBP heeft in 2001 de regelgeving rond de sociale zekerheid en met name de reïntegratie van de zieke werknemer met argusogen gevolgd. Sinds 1 januari 2002 hebben de eerste wijzigingen van de uitvoeringsstructuur hun beslag gekregen door de inwerkingtreding van de Wet SUWI (Structuur Uitvoering Werk en Inkomen). Het CBP adviseerde te zorgen voor grote transparantie en helderheid van de gegevensstromen. Het moet voor alle betrokken personen, instellingen en bedrijven duidelijk zijn welke informatie, tussen welke partijen voor welke doeleinden mag worden uitgewisseld. Dit kan worden bereikt door duidelijke regelgeving waarin met name de doelen van verstrekking afdoende gespecificeerd worden.

Het proces van reïntegratie bij arbeidsongeschiktheid wordt steeds vaker uitbesteed aan particuliere bedrijven. In verscheidene wetgevingsadviezen heeft het CBP de noodzaak benadrukt van specifieke regelgeving – bij voorkeur vastgelegd in wetgeving - voor de gegevensuitwisseling bij reïntegratie. De te reïntegreren werknemer verkeert in een kwetsbare positie en het gaat om medische gegevens. De evidente spanning tussen privacybelang en de belangen gemoeid met reïntegratie vragen om een oplossing voor de uitvoeringspraktijk. Hierin is nog niet voorzien.

Zorgtoewijzing

Toepassing van informatie- en communicatietechnologie is ook in de gezondheidszorg een trend naast de toename van regionale en landelijke elektronische registraties en van marktwerking. Wachtlijsten en zorgtoewijzing beheersten verder de discussie in de wereld van de gezondheidszorg. De gegevensverzameling en -verstrekking die daarbij een rol spelen, zijn buitengewoon privacygevoelig. In veel situaties bleek ook het medisch beroepsgeheim in het geding. De privacyrechten van patiënten dienen evenwel structureel beschermd te blijven. Het gezondheidsbelang van de patiënt laat deze anders geen ruimte om ook zijn privacybelang te laten gelden in een complexe, snel digitaliserende sector, die op zoek is naar efficiëntie en waar ook grote financiële belangen mee gemoeid zijn.

Doelen 2002

IN 2002 ZULLEN MET NAME DE VOLGENDE RESULTATEN WORDEN NAGESTREEFD:

- **Elektronische overheid**

De inzet van ICT kan de overheid toegankelijker, effectiever en klantgerichter maken, en de administratieve lasten voor bedrijven en instellingen terugdringen. Het CBP zal een visie publiceren op de privacyaspecten van deze ontwikkeling die kan bijdragen aan het vinden van kansrijke oplossingen en mogelijkheden tot verbetering.

- **Informatietechnologie in de zorg**

Ook in de gezondheidszorg zijn veranderingen gaande die ingrijpende gevolgen kunnen hebben voor de bescherming van de persoonlijke levenssfeer. Het CBP zal bijdragen aan een evenwichtige ontwikkeling op dit gebied door een publikatie over ICT in de zorg.

- **Onderzoek en statistiek**

Toenemende belangstelling voor resultaten en effecten leidt tot een grotere behoefte aan wetenschappelijk onderzoek en statistiek. Het CBP zal een kaderdocument uitbrengen waarin de wettelijke regels voor het gebruik van persoonsgegevens op dit gebied zullen worden verhelderd.

Digitale beelden van de openbare omgeving

Een bedrijf maakt op allerlei plaatsen in Nederland digitale opnamen van de openbare ruimte. De digitale opnamen geven een 360°-beeld van een bepaalde locatie. Een bepaald gebouw op die locatie kan dus ook op afstand bekeken worden. Daarvoor koppelt het bedrijf de digitale beelden aan andere gegevens: gemeente, plaats, straat, huisnummer en kadastrale coördinaten. De beelden geven van het gebouw een buitenaanzicht, met algemene informatie over de aard van het object en het gebruik daarvan.

Klanten van het bedrijf zijn onder andere woningcorporaties, nutsbedrijven, en gemeentelijke en provinciale overheden. Het is de bedoeling uiteindelijk te komen tot een optische basisregistratie van Nederland, die periodiek zal worden geactualiseerd en de bron vormt voor uiteenlopende toepassingen. Een aantal gemeenten heeft inmiddels met steun van het bedrijf een eigen optische basisregistratie aangelegd. Een prachtig systeem dat echter ook gebruikt wordt voor toepassingen waarvan eigenaren of bewoners directe gevolgen kunnen ondervinden.
Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon, moeten als persoonsgegevens worden beschouwd. Ook gegevens over objecten zijn soms persoonsgegevens. Dit is het geval als deze gegevens invloed kunnen hebben op de manier waarop een bepaalde persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. De Registratiekamer wees in 2001 het bedrijf op de privacy-aspecten van de ondernemingsactiviteit.
De eigenaren en bewoners van de betrokken panden kunnen in de regel zonder onevenredige moeite worden geïdentificeerd. Toepassingen waarbij digitale beelden worden gebruikt voor de beoordeling van individuele objecten en waarbij de betrokken eigenaren of bewoners directe gevolgen van deze beoordeling ondervinden (zoals bij taxatie en belastingen), zullen dan ook leiden tot het 'verwerken van persoonsgegevens'. Zowel de klanten als het bedrijf zelf zullen voor verschillende punten als 'verantwoordelijke voor de verwerking' van persoonsgegevens moeten worden aangemerkt. Het maken en mede met het oog op dergelijke toepassingen beschikbaar houden van digitale rondkijkbeelden, zal kunnen worden beschouwd als het 'verzamelen' van persoonsgegevens. De digitale beelden dragen immers vanaf het begin de mogelijkheid van een dergelijk gebruik in zich, terwijl de activiteiten van het bedrijf er uitdrukkelijk mede op gericht zijn te bevorderen dat een dergelijk gebruik plaatsvindt. Digitale 'rondkijkbeelden' van openbare ruimten en andere geo-informatie vallen dus voor een deel onder de privacywetgeving ●

- **Werknemers**

De privacy van werknemers is aan de orde bij een nieuwe versie van het rapport over controle op het gebruik van e-mail en internet op het werk, en van de privacychecklist voor ondernemingsraden. Ook zal de basis worden gelegd voor een publicatie over de positie van zieke werknemers.

- **Handelsinformatie**

Uit onderzoek is gebleken dat behoefte bestaat aan duidelijkheid over de verwerking van persoonsgegevens door handelsinformatiebureaus. Het CBP zal bevorderen dat binnen deze branche duidelijke normen voor een rechtmatige verwerking van persoonsgegevens worden vastgelegd.

- **Gebruik van telecommunicatie**

Het CBP zal een verkennend onderzoek doen naar de verwerking van persoonsgegevens over het gebruik van telecommunicatie. In eerste instantie gaat het daarbij vooral om afwikkeling van kosten ('billing'). De resultaten zullen aan de orde worden gesteld in een workshop met deskundigen en vertegenwoordigers van de sector.

- **Bijzondere politieregisters**

Het beheer van de politieregisters met 'criminele inlichtingen' behoeft verbeteringen waarbij zowel de privacybescherming als de opsporing van strafbare feiten zijn gebaat. Naast een versterking van het structurele toezicht op deze registers streeft het CBP naar een stroomlijning van de behandeling van verzoeken om inzage.

- **Openbaar register van WBP-meldingen**

Op de CBP-website zal een openbaar register van ontvangen meldingen voor iedereen toegankelijk worden. Naast een verbeterde versie van het WBP-meldingenprogramma op diskette zal ook de mogelijkheid worden geboden van een rechtstreekse aanmelding via internet.

- **Voorafgaand onderzoek**

De ervaringen die worden opgedaan bij het voorafgaand onderzoek naar verwerkingen met bijzondere risico's (artikelen 31-32 WBP) zullen op de CBP-website bekend worden gemaakt. Voor categorieën van veel voorkomende verwerkingen zullen, in overleg met direct belanghebbenden, waar mogelijk standaarden worden ontwikkeld.

- **Handhavingsplan**

Het CBP zal de voorwaarden ontwikkelen voor een systematische controle op de naleving van de meldingsplicht. Deze zullen samen met verschillende andere activiteiten op het terrein van toezicht, onderzoek en interventie worden vastgelegd in een handhavingsplan.