2000 in vogelvlucht

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

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

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

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

Informatieplicht aangescherpt

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

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

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

Doelbinding

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

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

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

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

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

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

Thema's

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

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

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

Belangrijkste publicaties

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

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

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

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

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

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

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

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

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

Actief op internationaal gebied

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

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

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

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

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

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

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

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