ICT en het recht om anoniem te zijn

januari 2000

/2/

ICT en het recht om anoniem te zijn

januari 2000

Inhoud

Voorwoord

Met het voorliggende advies beoogt de Raad voor het openbaar bestuur antwoord te geven op de adviesaanvraag van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties van 14 september 1999 over ‘ICT en privacy’. De digitalisering, horizontalisering en deterritorialisering van informatie heeft gevolgen voor het handelingsvermogen van de overheid. Over de wijze waarop de overheid dient om gaan met de gevolgen van bovengenoemde ontwikkelingen in relatie tot de bescherming van de privacy van de burger, is geadviseerd.

Dit advies is voorbereid door een werkgroep van leden uit de Raad voor het openbaar bestuur. De werkgroep bestond uit de volgende personen:
- prof. mr. P.F. van der Heijden (voorzitter);
- drs. P.J. Langenberg;
- mw. G.W. van Montfrans-Hartman;
- prof. dr. H.G. Sol;
- prof. dr. C.D. van der Vijver;
- mw. A.G.M. van de Vondervoort ;
- mw. dr. M.W.M. de Vries (projectsecretaris, geen Raadslid).

De Raad heeft ter voorbereiding van dit advies een expertmeeting over ‘ICT en privacy’ georganiseerd. De Raad spreekt waardering uit over deze bijeenkomst en bedankt de participanten voor hun bijdrage. Vanzelfsprekend komt de inhoud van dit advies geheel voor de verantwoording van de Raad.

Den Haag, januari 2000

Samenvatting

Informatie- en communicatietechnologie (ICT) vormt een steeds groter deel van onze economie. Digitalisering van informatie heeft invloed op de inrichting van de samenleving. Niet ICT in het algemeen, maar ICT-ontwikkelingen in relatie tot de privacy, vanuit oogpunt van burger en overheid, worden in dit advies bestudeerd. De Raad wil een aanzet geven de vragen hoe de overheid moet omgaan met ICT-ontwikkelingen in relatie tot privacy en wie verantwoordelijk is voor bescherming van de privacy, te beantwoorden. Betekent meer handelingsvermogen van de overheid door gebruik van ICT vanzelf minder privacy, of zijn er ook mogelijkheden om, door een andere wijze van omgaan met persoonsgegevens, meer handelingsvermogen te realiseren met evenveel of zelfs meer privacy?

Als norm wordt vooropgesteld dat privacy een recht van burgers is. Informatievrijheid betekent dat anderen geen informatie over ons kunnen inwinnen zonder onze toestemming of zonder dat daar een verplichting toe bestaat, en dat de informatiestroom die onszelf betreft ook door onszelf wordt beheerd. Burgers maken zich, ondanks dat privacy geen geïnstitutionaliseerd belang is, wel degelijk zorgen over hun privacy. Dit komt tot uiting in specifieke relaties tussen overheid en burger, en bedrijf en consument. Als voorbeelden van 'privacygevoelige' terreinen gelden: de gezondheidszorg, de sociale zekerheid, internet en de handhaving van de openbare orde en veiligheid. Burgers houden er individuele meningen op na over wat privacy-schending is en zijn tegelijkertijd bij verschillende gevallen bereid hun gegevens af te staan.

De Raad bestudeert de gevolgen van ICT-ontwikkelingen in de verzorgingsstaat en in de rechtsstaat. Door deze concepten te gebruiken en de verschillende taken van de overheid te onderscheiden, kan een goed beeld van overheid en burger in de informatiesamenleving worden gevormd.

De relatie tussen overheid en burger in de verzorgingsstaat en 'ICT en privacy' betreft de wisselwerking tussen het toepassen van ICT bij het uitvoeren en verbeteren van de overheidsdienstverlening en de bescherming van de persoonlijke levenssfeer van de burgers. Vooropgesteld staat volgens de Raad de algemene norm van informatievrijheid van de burgers. Daarom dient gebruik van persoonsgegevens aan betrokken burgers te worden gevraagd. De Raad erkent hierbij dat in sommige gevallen – zoals bij belastingen – het gebruik van persoonsgegevens eenvoudigweg een verplichting betreft. Specifieke criteria, ofwel de voorwaarden waaraan gegevensverwerking volgens burgers moet voldoen, zijn: duidelijkheid, doelbinding, transparantie en voorspelbaarheid. De overeenkomst tussen 'wat burgers willen' en de vereisten voor gegevensverwerking in het Wetsvoorstel over de Bescherming van Persoonsgegevens (WBP) komen nauw overeen.

Verschillende instrumenten kunnen door de overheid worden ontwikkeld om zowel haar handelingsvermogen als de privacy van de burger te vergroten. Het geven van gerichte voorlichting kan ertoe leiden dat de handelingsruimte van de overheid gelijk blijft of zelfs wordt vergroot, zonder dat de privacy van de burgers wordt geschonden. Een ander instrument voor de overheid is om bij gegevensverwerking tussen instanties geen gegevens door te geven, maar te laten uitzoeken wie aan bepaalde criteria voldoen. Dit wordt 'ontkoppeld koppelen' genoemd. Bij pro-actieve dienstverlening wordt door het koppelen van bestanden en het selecteren op basis van bijvoorbeeld inkomensgegevens, door de overheid 'voor ons gedacht'. Dit kan als een inbreuk worden gezien op de privacy. De vraag of 'een burger niet discreet in armoede mag leven' is volgens de Raad in het kader van de privacy een legitieme vraag. De angst voor een alles registrerende overheid en voor paternalisme kan volgens de Raad worden weggenomen door een gedifferentieerd systeem voor pro-actieve dienstverlening. Hierbij kan een burger zelf aangeven waarvoor hij wel of niet in aanmerking wil komen. Dit kan een vanzelfsprekende gang van zaken worden in gevallen waarbij 'het ontvangen van dienstverlening geen verplichting vormt'.

Voor het praktische ontwerp van de informatiehuishouding zijn verschillende alternatieven mogelijk. Een aanpak waarbij wordt uitgegaan van decentrale gegevensbanken en verwijsindices kan zowel de efficiency als de effectiviteit van overheidsbeleid ten goede komen en tegelijkertijd een goede waarborg vormen voor de privacy van de burger. Ditzelfde kan echter ook worden gezegd van landelijke gegevensbanken en bovensectoraal gebruik van persoonsnummers, mits die zorgvuldig zijn ingericht. Bij het inrichten van informatie-infrastructuren dienen de eerder genoemde normen het uitgangspunt te vormen en is zorgvuldige omgang met gegevens en zorgvuldig toekennen van autorisaties van groter belang dan de vorm van de informatiehuishouding.

'ICT en privacy' komt bij de taak van de overheid in de democratie tot uiting bij voorstellen voor elektronisch stemmen. Deze ontwikkeling wordt door de Raad ondersteund, maar dient met de nodige behoedzaamheid te worden uitgevoerd.

De functie van de overheid in de rechtsstaat is het waarborgen van de individuele vrijheid van haar burgers. ICT-wetgeving samen met omgangsvormen die door marktwerking ontstaan, vormen de basis voor de omgang met privacy op internet. De Raad is van mening dat veiligheid van communicatie en transacties via internet primair voor rekening moet komen van gebruikers en aanbieders. De Raad ondersteunt hierbij het streven naar anonimiteit en zelfredzaamheid van de gebruiker.

Het verwerken van persoonsgegevens kan ook geschieden met het doel profielen te creëren. Technieken voor het maken van profielschetsen van

groepen burgers of klanten, zoals *datamining*, kunnen indien succesvol behalve klantenprofielen ook informatie opleveren over potentiële kopers, riskante verzekerden, potentiële fraudeurs bij de belastingdienst of potentiële rechthebbenden op een subsidie. Op basis van de uitkomsten van het creëren van profielen kunnen gedragingen als uitsluiting (geen abonnement of verzekering krijgen), risicoselectie (bij hypotheekverstrekking of verzekeringen) of informatiestalking (direct-marketing activiteiten) ontstaan. Het maken van profielschetsen en het toerekenen van een profielschets is onder bepaalde voorwaarden toegestaan. Het gemaakte profiel mag echter geen reden zijn voor negatieve besluitvorming over een persoon zonder menselijke tussenkomst. Door deze laatste toevoeging in de WBP wordt het risico van het maken van profielen danig verkleind.
De privacy van een burger of een consument kan ondanks goede regelgeving toch worden geschonden. Daarom pleit de Raad voor het invoeren van een boete op privacyschendingen. De Raad beoordeelt voorstellen voor bestuursdwang, strafrechtelijke sancties en de mogelijkheid voor schadevergoedingen positief.

Zowel grondrechten, privacywetgeving (WBP) en ander (inter)nationaal recht worden aangepast aan de veranderende omstandigheden. ICT-ontwikkelingen kunnen tot geheel nieuwe vragen leiden, waardoor nieuwe wetgeving moet worden gemaakt. Het uitgangspunt bij nieuwe wetgeving of aanpassingen van bestaande wetgeving is de wetgeving zoveel mogelijk techniek-onafhankelijk te maken. Hierbij lijkt het de Raad vanzelfsprekend dat gedragingen die strafbaar zijn in het fysieke leven, dat ook zijn op internet. De opkomst van ICT brengt ook zijn eigen criminaliteitsbeeld en eigen opsporingsmethoden met zich. Het binnendringen van computers of netwerken door *hackers*, het plegen van digitale creditcardfraude, het illegaal binnenhalen van betaaltelevisie en uitingsdelicten zoals kinderpornografie op het net, zijn hiervan voorbeelden. Een nieuwe opsporingsmethode is bijvoorbeeld het volgen van de verblijfplaats – *tracking and tracing* – van een mobiele telefoon. Voor zowel nieuwe delicten als nieuwe opsporingsmethoden geldt dat wat strafbaar of toelaatbaar is, onafhankelijk dient te zijn van de technische toepassing.
Met betrekking tot opsporing van internetdelicten is het beveiligen van verkeer via internet een belangrijk thema. Omdat de overheid voor bijvoorbeeld de staatsveiligheid berichten wil kunnen onderscheppen, is een bovengrens gesteld aan versleuteling (geheimtaal). De Raad is echter van mening dat een bovengrens op cryptografie niet het juiste antwoord op de afweging privacy versus veiligheid is.

1.
ICT en privacy nader beschouwd

Onlangs is een meisje uit het Oosten van Nederland in het holst van de nacht het ouderlijk huis uitgeslopen. De duisternis trotserend is ze zonder bericht achter te laten naar het Westen vertrokken om zich bij haar geliefde te vervoegen. In de daarop volgende dagen werden haar ouders ongeruster en ongeruster en uiteindelijk meldden ze de verdwijning bij de politie. Romeo en Julia leefden intussen hun gedroomde leven en hoewel de liefde in veel voorziet, ze vult de maag niet. De behoefte aan cash nam toe, een geldmachine bood uitkomst, maar werd hen tenslotte ook fataal. De geïnstalleerde videocamera registreerde feilloos het prille geluk. De jongen werd herkend vanwege een eerdere misstap en even later was de locatie van de geliefden bekend. De Amsterdamse politie maakte abrupt een einde aan de romance. Ouders en politie gelukkig, maar middels oneigenlijk gebruik van de camera is het geluk van Romeo en Julia, en eventueel nageslacht, in de kiem gesmoord.
Uit: Metro, 21 december 1999, column van Joost Engelberts, 'Big Brother niet alleen maar op TV'.

1.1
Inleiding

In het WRR rapport *Staat zonder land* van 1998 staat het afnemende handelingsvermogen van de overheid als gevolg van een afnemende binding met een bepaald grondgebied als gevolg van ontwikkelingen in de informatie- en communicatietechnologie (ICT) centraal.[1] De politiek filosoof Van Gunsteren spreekt van een overgangstijd en van *de ongekende samenleving* wanneer hij laat zien dat huidige ontwikkelingen niet volgens de bestaande besturingskaders te verklaren zijn.[2] We zijn nauwelijks in staat de problemen en ontwikkelingen van deze tijd aan te pakken. Hiervoor zijn nieuwe percepties en begrippenkaders nodig. Ook de vice-voorzitter van de Raad van State, de heer Tjeenk-Willink, onderkent dit en spreekt over de overheid die pluricentristisch is geworden.[3] Niet alleen zien we een afnemende rol en invloed van de overheid door ICT-ontwikkelingen, maar ook door een grotere rol van andere (internationale) overheden. Deze afnemende invloed wordt onder andere veroorzaakt doordat ICT-ontwikkelingen sneller gaan dan de overheid erop kan reageren. Dit zien we met name bij het aanpassen van wetgeving op nieuwe ICT-ontwikkelingen. Ook is de overheid niet langer

---

1 WRR, 1998.
2 Gunsteren Van, 1994.
3 Tjeenk-Willink, 1999.

almachtig, maar één van de spelers in een ingewikkeld veld van interacties en betrekkingen.

Uit zowel wetenschappelijke hoek als de beleidspraktijk wordt onderkend dat ICT-ontwikkelingen grote invloed hebben op de inrichting van de samenleving. Er lijkt meer aan de hand te zijn dan betere technologische technieken om dezelfde dingen te regelen. De nieuwe technieken hebben nieuwe vragen opgeroepen. Een belangrijk *issue* is de ontwikkeling van ICT en de invloed hiervan op privacy van de burgers.

Niet de consequenties van de digitale samenleving in het algemeen, maar specifiek de verhouding tussen het gebruik van ICT en de bescherming van de persoonlijke levenssfeer staat centraal in dit advies. Hierbij geldt dat de overheid uiteenlopende taken heeft en daarbij verschillend omgaat met 'ICT en privacy'. De overheid in haar verzorgende functie gebruikt ICT voor dienstverlening. Zij onderkent dat gebruik van persoonsgegevens aan bepaalde wettelijke en informele regels omtrent privacybescherming moet voldoen. De overheid in haar rol als handhaver van de openbare orde onderkent bovengenoemde ook, maar heeft een voorkeur voor zo min mogelijk beperkingen op het gebruik van gegevens. De wensen van de burgers zijn ook niet eenduidig. In bepaalde relaties tot de overheid zijn burgers gesteld op hun privacy zoals bijvoorbeeld een burger in relatie tot een sociale dienst. Tegelijkertijd zijn burgers bereid hun persoonsgegevens te verkopen voor een kortingskaart, overschaduwt veiligheid de behoefte aan privacy, kunnen er geen camera's genoeg worden geplaatst en vergaapt een deel van het volk zich collectief aan het televisie-programma *Big Brother*.

In dit advies worden ICT-ontwikkelingen in relatie tot de privacy vanuit het oogpunt van burger en overheid bestudeerd. De Raad wil een aanzet geven de vragen hoe de overheid moet omgaan met ICT-ontwikkelingen in relatie tot privacy en wie verantwoordelijk is voor de bescherming van privacy, te beantwoorden.
Ondanks het streven naar een algemene visie dient niet uit het oog te worden verloren dat elk aan ICT-gerelateerd advies tijd- en plaatsgebonden is. De normen voor omgang met privacy worden in dit advies zoveel mogelijk techniek-onafhankelijk, dus 'los van de tijd' geformuleerd. Echter, de normen over privacy betreffen in Nederland levende normen. Waar in Nederland burgers zich zorgen maken over hun privacy, is privacy in de Verenigde Staten of in Japan geen onderwerp van discussie. Bovendien geldt dat de ICT-ontwikkelingen sneller gaan dan de 'drukpers' en dat wellicht bij het verschijnen van dit advies, nieuwe ICT-mogelijkheden alweer nieuwe vragen hebben opgeroepen.

Het gebruik van ICT door de overheid, in het bijzonder de verbetering van de dienstverlening en de mogelijkheden voor actieve en directe participatie van de burger in de politiek, zijn reeds beschreven in een tweetal adviezen van de

Raad. In het advies van april 1998 *Dienen en verdienen met ICT* zijn de mogelijkheden voor verbetering van de overheidsdienstverlening met gebruik van nieuwe technologie besproken. In het tweede ICT-advies van de Raad van december 1998 *De grenzen van de internetdemocratie* zijn de kansen en bedreigingen van het gebruik van internet voor het publieke debat en voor politieke besluitvorming in een representatieve democratie bestudeerd.

In dit advies zal vanuit het perspectief van de verschillende belangen van burgers en overheid – en soms tussen burgers en overheid – de digitale samenleving worden bestudeerd. De WRR spreekt van een afnemend handelingsvermogen van de overheid, maar vraagt zich af of de ICT-ontwikkelingen ook kunnen worden benut om de doelmatigheid van het overheidsbeleid te vergroten. Wellicht is dit mogelijk, maar verhoogde beleidsambities kunnen ook botsen met beginselen zoals privacy. In de adviesaanvraag staat de wisselwerking tussen gebruik van 'ICT en privacy' centraal.

De kernvragen luiden:
- Welke verschillende opties bestaan er voor de overheid om binnen het kader van de toekomstige Wet Bescherming Persoonsgegevens in het algemeen om te gaan met het privacybegrip (bijvoorbeeld persoonsnummers) en wat betekent dit voor het handelingsvermogen van de overheid?
- Betekent meer handelingsvermogen vanzelf minder privacy of zijn er ook mogelijkheden om door een andere wijze van omgaan met persoonsgegevens meer handelingsvermogen te realiseren met evenveel of zelfs meer privacy?
- Welke posities hebben basisregistraties in de overheidsinformatiehuishouding ten opzichte van sectorale indexen die zich ontwikkelen tot centrale registers met algemene gegevens?

Bovenstaande vragen zullen in het brede kader over het beleid van de overheid ten aanzien van 'ICT en privacy' worden beantwoord.

1.2
Privacy

Het recht op privacy zoals in artikel 10 van de Grondwet beschreven: "ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer", is een ruim concept. Het is een concept dat aan 'individuele vrijheid' gestalte geeft. Deze definitie is ambigu maar privacy is moeilijk specifieker te definiëren omdat het een contextgebonden, relationeel en bovendien relatief begrip is.[4]

De persoonlijke vrijheid is contextueel bepaald; de vrijheid van een individu is in een democratische rechtsstaat groter dan in een totalitair regime. Zij is relationeel; een individu vindt de aantasting van zijn persoonlijke integriteit

[4] Gutwirth, 1998.

kleiner als een arts zijn medische gegevens krijgt, dan wanneer een verzekeringsmaatschappij of zijn buurman hierover beschikt. Dit relationele aspect van privacy blijkt in grote mate te verklaren waarom privacy geen politiek strijdpunt is. Slechts in relatie tot bepaalde vraagstukken blijken burgers zich zorgen te maken over privacy.
Privacy is bovendien een relatief ofwel een persoonlijk begrip. Er zijn mensen met grote behoefte aan anonimiteit, die hun privacy beschermen door geen adresgegevens te verstrekken voor bijvoorbeeld een klantenkortingskaart, terwijl er ook mensen zijn die hun meest intieme persoonlijke zaken bespreken in eigentijdse talkshows.
Vervolgens blijkt privacybeleving een tijdgebonden concept te zijn. In de zeventiger jaren waren burgers bang voor *Big Brother* en keerde zich massaal tegen het voorstel een volkstelling te houden. In de huidige maatschappij is het vanzelfsprekend om ingeschreven te staan in de Gemeentelijke Basisadministratie (GBA) en wordt cameratoezicht ter bevordering van de veiligheid in openbare ruimten ook als vanzelfsprekend ervaren.

In dit betoog over de gevolgen van ICT-ontwikkelingen voor de privacy ligt de nadruk op informationele privacy. Met deze privacy wordt de bescherming van de persoonlijke vrijheid met betrekking tot het gebruik van persoonsgegevens bedoeld. De Ruiter beschrijft de volgende tegenstrijdige belangen: "Enerzijds zijn er fundamentele rechten en vrijheden van de mens in het geding. Men heeft rekening te houden met het concrete belang van de individuele burger en consument die in het alledaagse leven zicht en greep wil houden op zijn persoonsgegevens, zodanig dat hij vertrouwen kan hebben in de maatschappelijke omgang met deze gegevens. Anderzijds is , …, een zekere mate van informatievrijheid als grondslag van de inrichting van onze samenleving onontbeerlijk. Voor een goed functionerende verzorgingsstaat, voor de doelmatigheid van het maatschappelijk handelen, en voor de bestrijding van fraude en criminaliteit, zijn kennis en gebruik van persoonsgegevens noodzakelijk".[5] Deze belangenstrijd wordt, zowel op het niveau van de verzorgingsstaat – relatie overheid en burger – als op het niveau van de rechtsstaat – relatie overheid en burger en de relatie tussen private partners – als in de democratie, in dit advies uiteengezet.

Een belangrijk uitgangspunt in dit advies is dat privacyschending onafhankelijk is van technologie. In de beleving van burgers kan er desondanks wel een verschil bestaan tussen digitale en fysieke informatiestromen, en kan hierbij het digitale verkeer de beleving van privacy beïnvloeden. Maar in principe geldt dat wat in dit advies wel of geen schending van privacy wordt geacht, niet wordt veroorzaakt door techniek. Natuurlijk zorgen ICT-ontwikkelingen voor nieuwe vraagstukken en mogelijke schendingen van privacy, maar beslissingen over de toelaatbaarheid van het gebruik van persoonsgegevens

---

[5] Ruiter De, 1998, p. 287.

behoren en zullen in dit advies onafhankelijk van de techniek worden genomen.

1.3
ICT-ontwikkelingen

Informatieproducten krijgen tegenwoordig een steeds grotere economische betekenis. Zowel bedrijven als dienstverleners in de informatiesector vormen een steeds groter deel van ons bruto nationaal product. Denk hierbij aan producenten van informatie- en communicatietechnologie, aanbieders van telecommunicatie- en softwareproducten, aanbieders van informatiediensten, consultants, adviseurs etc. Informatie- en communicatietechnologie kenmerkt zich door digitale technologie en geheugenchips die steeds kleiner worden en steeds meer informatie kunnen opslaan. Ook nemen we steeds meer draadloze communicatie waar.

Een korte beschrijving van de belangrijkste gevolgen van de toename van ICT is nodig om de relevantie van deze ontwikkelingen in relatie tot de bescherming van de informationele privacy te doorzien. De volgende kenmerken van de opkomende informatiemaatschappij zijn van belang.[6]

- *Deterritorialisering*; informatie, bijvoorbeeld op internet, is niet langer aan tijd en plaats gebonden en dus niet langer binnen de grenzen van één staat onder te brengen. Hierdoor worden staten gedwongen tot bestuurlijke en wettelijke afstemming van beleid. Een voorbeeld hiervan is de vraag naar de rechtspositie van een internetbedrijf dat fysiek opereert vanuit Nederland, maar waarbij de provider is gestationeerd op een eilandje in de Stille Zuidzee.
- *Turbulentie*; nieuwe technieken en toepassingen op het terrein van ICT volgen elkaar sneller op dan de maatschappelijke gevolgen ervan kunnen worden overzien, en sneller dan de formele wetgeving kan worden aangepast. Hierbij kan worden gedacht aan de mogelijkheid de plaats van mobiele telefoons te traceren zonder dat hiervoor al wetgeving bestaat.
- *Horizontalisering*; de toename van ICT leidt tot een verandering in organisatiestructuren. Hiërarchische relaties worden vervangen door netwerken waarbij eenieder met een computer toegang heeft tot bepaalde gegevens. Dit kan leiden tot privacyschending wanneer blijkt dat door de horizontaliserering meer mensen dan oorspronkelijk de bedoeling was ‘in een databank kunnen kijken’. Het voorbeeld van rondslingerende ‘wachtwoorden’ binnen organisaties waar met persoonsgegevens wordt gewerkt, is geen unicum.
- *Dematerialisering*; ook wel digitalisering genoemd. Informatie en kennis – belangrijke economische hulpbronnen – zijn meer en meer niet in tastbare vorm maar digitaal aanwezig. Hierdoor is de bron van de informatie vaak moeilijk te traceren en moeilijk te controleren.

---

[6] Bovens, 1999.

- *Transparantie*; automatisering en het koppelen van bestanden kan de doorzichtigheid van systemen vergroten. Deze transparantie kan leiden tot betere dienstverlening. Tegelijkertijd zijn nieuwe technieken, zoals encryptie, ontstaan die dienen ter bescherming van de privacy, waardoor de transparantie weer afneemt.

1.4
Conceptueel kader

In dit advies over 'ICT en privacy' wordt als norm vooropgesteld dat privacy van burgers een recht is. Ook vrijheid van informatie – de informationele privacy – heeft betrekking op de persoonlijke levenssfeer. Mensen zijn tot op zekere hoogte vrij te bepalen welke informatie zij over zichzelf met anderen delen. Informatievrijheid betekent dat anderen geen informatie over ons kunnen inwinnen zonder onze toestemming of zonder dat daar een verplichting toe bestaat, en dat de informatiestroom die onszelf betreft ook door onszelf wordt beheerd. Een uitzondering op basis van een verplichting vormt bijvoorbeeld de belastingdienst. De overheid heeft op grond van specifieke functies, in het voorbeeld van de belastingdienst gezien haar herverdelende functie, het recht informatie van haar burgers te gebruiken. Ondanks deze uitzonderingen geldt in een fatsoenlijke samenleving dat het maatschappelijk onaanvaardbaar is wanneer burgers niet weten wie, welke informatie, waar, wanneer en hoe over hen verwerken.[7] Privacybescherming betreft dus de waarborg van de individuele autonomie van burgers.

Bovenstaande betekent niet dat elk gebruik van informatie of persoonsgegevens een schending van de privacy is, wel staat buiten discussie dat burgers in principe eigenaren van hun eigen gegevens zijn. Dit 'zelf eigenaar zijn van je gegevens' geldt met inachtneming van enkele uitzonderingen (in het kader van de verzorgende of opsporende en handhavende functies) in relatie met de overheid, en is een onbetwistbaar recht van een mens in relatie tot de private sector. Voordelen van het gebruik en dus het afstaan van gegevens worden vanzelfsprekend in dit advies onderkend, maar beslissingen over het gebruik van informatie dienen in een maatschappelijke dialoog met betrokkenen te worden gemaakt.

1.4.1
Verschillende burgers, verschillende waarden

Het beschrijven van normen voor goede omgang met 'ICT en privacy' is gecompliceerd, omdat er niet één burger of één overheid is. Alvorens dieper in te gaan op 'privacynormen' worden de verschillende perspectieven van overheid en burgers met betrekking tot ICT besproken.

Voor het perspectief van de burger is een onderzoek naar de privacybeleving

---

[7] Hamelink, 1999.

van burgers in de informatiemaatschappij van het Rathenau Instituut bestudeerd.[8] Vervolgens zijn secundaire bronnen gebruikt, dat wil zeggen artikelen waarin door 'experts' wordt beschreven wat burgers denken of verwachten, en heeft de Raad vertegenwoordigers uit zowel overheidssfeer, wetenschap als commercie geraadpleegd.[9]

In het onderzoek van het Rathenau Instituut dat is gehouden in opdracht van het Platform voor Wetenschap en Ethiek is op basis van interviews, groepsgesprekken en schriftelijke enquêtes onderzoek gedaan naar de privacybeleving van burgers. Op basis van de schriftelijke vragenlijst (294 respondenten) blijkt dat de helft van de burgers zich wel eens in een situatie vindt verkeren waarin zij zich in hun privacy voelen aangetast. Burgers zijn volgens dit onderzoek grofweg in drie groepen in te delen:

1. burgers die van mening zijn dat informatietechnologie nodig is in de huidige maatschappij en die daar geen privacyproblemen van ondervinden (19%);
2. burgers die vinden dat het toenemende gebruik van informatietechnologie privacyproblemen met zich meebrengt, maar die echter ook van mening zijn dat de huidige maatschappij niet meer zonder informatietechnologie kan functioneren (35%);
3. burgers die van mening zijn dat de informatietechnologie een bedreiging vormt voor de privacy en dat dit in veel gevallen zou moeten zijn te voorkomen. Het gebruik van de informatietechnologie is volgens hen niet altijd noodzakelijk (47%).[10]

De belangrijkste bevinding uit de individuele interviews van het Rathenau Instituut is dat mensen privacyaantasting verschillend ervaren. Het is niet zo dat iemand die privacygevoelig is alle genoemde voorbeelden even sterk als aantasting van zijn privacy beoordeelt.[11] "Privacy is kennelijk een begrip

---

[8] Smink, e.a., 1999.

[9] Een voorbeeld van een secundaire bron is het verslag van Van Linschooten uit het Hengelo's Informatie Team sociale voorzieningen. "Volgens Van Linschooten zijn de meeste mensen wel positief". In: 'In Hengelo komt de subsidie naar je toe'. NRC 28-08-1999.
De raadpleging van burgers door de Raad heeft plaatsgevonden in een expertmeeting over 'ICT en privacy'.

[10] Smink, e.a., 1999.

[11] De privacygevoeligheid is onderzocht bij de volgende voorbeeldsituaties: – in een kledingzaak uw postcode + huisnummer afgeven na het afrekenen, – meedoen aan een telefonische enquête, – een postorderbedrijf dat uw kredietwaardigheid controleert bij het BKR in Tiel, – opgenomen worden door een camera bij een benzinepomp, – ontvangen van een 'blije doos' bij de geboorte van een kind, – het inleveren van een kopie van uw paspoort bij uw werkgever, – afgeven van een geneeskundige verklaring voor aanvraag rijbewijs, en – meedoen aan een anonieme schriftelijke enquête over privacy. Smink, e.a., 1999.

waarbij ieder een eigen combinatie van waarden hanteert".[12]

In de *expertmeeting*, georganiseerd door de Raad, was één van de vragen hoe volgens burgers wordt gedacht over privacy. Privacy is immers geen politiek strijdpunt waarop politieke partijen zich duidelijk onderscheiden. De conclusie was hier ook dat privacy wel degelijk een *issue* is waar burgers zich zorgen over maken. Dit probleem komt alleen niet tot uiting als een geïnstitutionaliseerd belang, maar komt in specifieke relaties tussen overheid en burger, of bedrijf en consument aan de orde. Als voorbeelden van 'privacygevoelige' terreinen gelden: de gezondheidszorg, de sociale zekerheid, internet en de handhaving van de openbare orde en veiligheid. De conclusies uit de *expertmeeting* komen sterk overeen met de bevindingen van het Rathenau Instituut en de secundaire literatuur.

Privacy is dus een belangrijk maatschappelijk *issue*. Dit blijkt niet alleen uit bovenstaande gevolgtrekkingen of uit de veelheid van artikelen en zelfs specifieke tijdschriften zoals 'Privacy en Informatie' die over dit onderwerp worden gepubliceerd, maar tevens uit de grote stroom privacygerelateerde wetgeving en de ontwikkeling van sectorale privacyprotocollen.[13] Anderzijds, zijn er ook maatschappelijke belangen die een groter gewicht krijgen dan de bescherming van de privacy. In Binnenlands Bestuur van 29 oktober 1999 zegt Visser het volgende over veiligheid en privacy: "Het privacyargument verbleekt bij het gevaar van een mes tussen je ribben".

De belangen van betrokkenen zijn divers. Een burger heeft niet alleen betrekkingen met de overheid maar is ook consument en soms producent. Deze burger kan zich enerzijds zorgen maken over privacy, maar is anderzijds ook bereid haar privacy te laten schenden wanneer hij of zij er baat bij heeft. Deze schending kan worden toegestaan omdat een burger er individueel belang bij heeft (*airmiles*), of omdat het hoort bij de uitoefening van een specifieke taak (in de dienstverlenende sfeer van de overheid, zoals uitvoering van de bijstand), of omdat het gebeurt in het algemeen belang bijvoorbeeld wanneer er sprake is van een maatschappelijk probleem zoals bezorgdheid over veiligheid.

1.4.2
De overheid: verschillende taken, verschillende belangen

Vanuit het perspectief van de overheid is de relatie tussen 'ICT en privacy' ook complex. De overheid heeft een veelzijdige rol. Zij is gebruiker van gegevens, regelgever en wetgever, en handhaver van openbare orde en veiligheid. Als

---

[12] Smink, e.a., 1999, p. 60.

[13] Wetgeving: het wetsvoorstel Wet bescherming persoonsgegevens; wet op de computercriminaliteit, OESO privacyrichtlijn, herziening digitale grondrechten etc. Een voorbeeld van een privacyprotocol is de CVCS Privacy Almanak (Stichting CVCS, 1999) waarin omgang met privacy in de sociale zekerheidssector wordt uitgewerkt.

gebruiker van gegevens is zij actief in haar functie van dienstverlener in de verzorgingsstaat, maar tevens als handhaver van orde en veiligheid in de rechtsstaat. Als regelgever opereert zij in haar rol als rechtsstaat en is zij ook degene die verantwoordelijk is voor het ontwikkelen en handhaven van wetgeving.

De verschillende functies van de overheid vormen het conceptueel kader voor dit advies. Hiermee is helder dat we niet over de overheid 'als ware het één entiteit' kunnen spreken. In veel publicaties over de rol van de overheid inzake ICT-ontwikkelingen ligt de nadruk op de rol van de overheid in de verzorgingsstaat en op mogelijkheden van ICT voor het publieke debat. Om de handelingsruimte van de overheid inzake 'ICT en privacy' volledig te bestuderen, worden in dit advies twee staatkundige concepten die nauw met elkaar zijn verweven, uit elkaar gehaald. We bestuderen de gevolgen van ICT-ontwikkelingen in de verzorgingsstaat en de rechtsstaat. Door deze concepten te gebruiken en de taken van de overheid op deze terreinen te onderscheiden, kan een compleet beeld van de rol van de overheid in de informatiesamenleving worden gevormd.

De Raad is van mening dat, gezien de norm van informatievrijheid, burgers primair zelf dienen te bepalen welke informatie zij over zichzelf met anderen delen. Daarom kunnen niet gemakkelijk vanuit overheidswege normen voor de omgang met de privacy worden opgesteld. Het gewoonweg bepalen dat informatieverwerking nodig is voor het uitvoeren van een dienst, is niet voldoende reden voor gebruik van gegevens. Om de privacy van burgers te waarborgen en tegelijkertijd ruimte te bieden voor overheidsoptreden en gebruik van ICT, worden in dit advies verscheidene richtlijnen opgesteld. Daarbij wordt uitgebreid ingegaan op het wetvoorstel voor de bescherming van persoongegevens. De vereisten in deze wet blijken nauw overeen te komen met de omgangsvormen die in dit advies worden beschreven. Deze criteria betreffen onder meer duidelijkheid, doelbinding, transparantie of voorspelbaarheid en zeggenschap. Duidelijkheid vereist dat gegevens alleen mogen worden verwerkt voor een van te voren gespecificeerd en gerechtvaardigd doel. Doelbinding sluit aan bij het gegeven dat burgers in sommige situaties wel, en in andere situaties zich geen zorgen maken over de privacy. Ook voorspelbaarheid komt tegemoet aan de wensen van de burgers. Indien gegevensverwerking voorspelbaar is, hebben burgers minder snel het 'gevoel' dat hun privacy wordt geschonden. Zeggenschap wordt in de WBP vertaald in het recht op verzet en informatieplicht bij verwerking van persoonsgegevens[14] en sluit nauw aan bij de norm over informatievrijheid.

Vooropgesteld staat dus, met inachtneming van uitzonderingen, het principe van de informatievrijheid ofwel informatie-autonomie van de burgers. Als

[14] Zie paragraaf 2.2.

vervolgens is voldaan aan de criteria duidelijkheid, doelbinding en transparantie en gegevens mogen worden verwerkt, dient de gebruiker en dus ook de overheid als instrument 'minimalistisch gegevensbeheer' toe te passen. Dit wil zeggen dat de gebruiker bij het uitvoeren van beleid steeds dient uit te gaan van een zo minimaal mogelijk gebruik van gegevens. Bij informatie-uitwisseling leidt dit in sommige gevallen tot ontkoppeld koppelen in plaats van het doorgeven of koppelen van gegevens.[15]

Omdat privacyvrijheid van het individu centraal staat, geldt als laatste vereiste dat het schenden van privacy niet gratis is. Als het schenden van privacy 'onbestraft' blijft, betekent de autonomie van de burgers in de praktijk immers niet zo veel. Voorstellen voor het opleggen van boetes en schadevergoedingen bij privacyschendingen sluiten nauw aan bij het uitgangspunt van individuele informatie-autonomie.[16]

In de inleiding werd reeds geschetst dat over de vraag hoe de overheid moet omgaan met ICT-ontwikkelingen in relatie tot privacy en over de vraag wie verantwoordelijk is voor de bescherming van de privacy, zal worden geadviseerd. Omdat de overheid verschillende rollen vervult, blijkt de vraag hoe de overheid moet omgaan met 'ICT en privacy' complex te zijn. Bovendien is de overheid maar één van de actoren in onze samenleving. Bij de ICT-ontwikkelingen zijn ook commerciële bedrijven en andere (internationale) overheden betrokken. Hierdoor wordt het tweede deel van de vraag relevant. Wie is wanneer verantwoordelijk voor de bescherming van de privacy? Als een burger over internet surft, is deze burger dan zelf verantwoordelijk voor zijn privacy of ligt hier een regulerende taak voor de overheid? Op bovenstaande vragen wordt in dit advies antwoord gegeven.

1.5
Leeswijzer

In dit *eerste hoofdstuk* zijn de begrippen ICT en privacy uiteengezet en is het conceptueel kader weergegeven.
In het *tweede hoofdstuk* komt het functioneren van de overheid met betrekking tot 'ICT en privacy' in de verzorgingsstaat aan de orde. Deze functie bevat overheidstaken die gericht zijn op het, in een betrekkelijk vrije markteconomie, reguleren van collectieve goederen en het garanderen van een minimum-bestaans- en verzorgingsniveau voor alle burgers. 'ICT en privacy' betreft hier

---

[15] Zie paragraaf 2.3.5. Ontkoppeld koppelen houdt in dat wanneer de ene instantie gegevens van een andere instantie nodig heeft, de laatstgenoemde de gegevens niet 'doorgeeft', maar uitzoekt wie aan bepaalde criteria voldoet en die informatie doorgeeft. Dus in plaats van complete files over en weer te sturen, wordt een lijstje gestuurd met bijvoorbeeld 'de volgende burgers uit deze gemeente voldoen aan het criterium salaris onder 50.000 gulden per jaar'.

[16] Zie paragraaf 3.4.

voornamelijk de wisselwerking tussen het toepassen van ICT bij het uitvoeren en verbeteren van de overheidsdienstverlening – zoals het koppelen van bestanden en het toepassen van pro-actief beleid – en de bescherming van de persoonlijke levenssfeer van de burgers.

In paragraaf 2.2 wordt de dienstverlenende rol van de overheid beschreven. Sectorale belangen van burgers met betrekking tot privacy als wel de relatie tussen gebruik van gegevens en de nieuwe privacywetgeving (ontwerp Wet bescherming persoonsgegevens) komen aan de orde. Hierbij zullen op grond van de norm informatievrijheid, begrippen als doelbinding, transparantie en terughoudendheid in het gebruik van persoonsgegevens de leidende principes zijn.

In de volgende paragraaf komt de informatiehuishouding van de overheid aan de orde. Voor dienstverlening zijn data nodig en verwerking van gegevens moet voldoen aan een aantal wettelijke regels. Dit zegt echter nog niet wat de 'beste' of meest 'privacybeschermende' manier is van databeheer. De vraag naar een '*best practice*' voor de inrichting van de informatiehuishouding wordt in deze sectie beantwoord.

Paragraaf 2.4 gaat in op de mogelijkheid om elektronisch te stemmen. Voorstanders van invoering van elektronisch stemmen hebben voor dit doel een Platform Elektronisch Stemmen (PELS) opgericht. Hierbij wordt verondersteld dat privacy voornamelijk een technisch *issue* is. Ook bij elektronisch stemmen moet de mogelijkheid om anoniem te stemmen gewaarborgd blijven. Een burger moet maximaal een keer kunnen stemmen en de inhoud van de stem mag niet te achterhalen zijn. Gebruik van cryptografie kan dit mogelijk maken.

In *hoofdstuk drie* wordt 'ICT en privacy' in de rechtsstaat bestudeerd. Deze functie van de overheid is niet alleen een andere dan de functie in hoofdstuk twee, maar vertegenwoordigt tevens op zichzelf al een dubbelrol. In de rechtsstaat kan de overheid worden beschouwd als zowel wetgever als handhaver. In het kader van de handhaving is zij zowel beschermer (voor de handhaving van privacywetgeving) als gebruiker van onze gegevens (voor de handhaving van openbare orde en veiligheid). In dit hoofdstuk komt ook de vraag wie verantwoordelijk is voor bescherming van de privacy nadrukkelijk aan de orde. Moet de overheid omgangsnormen maken voor 'ICT en privacy', of kan zij dat beter aan de markt overlaten?

In paragraaf 3.2 wordt ingegaan op de digitale snelweg (zo men wil de digitale landweg). Communicatie over internet is nog niet voldoende beveiligd. De vraag wie hiervoor verantwoordelijk is en de regelgeving over cryptografie (een beveiligingstechniek) wordt besproken.

In de volgende paragraaf komt het zoeken naar profielen op basis van onderzoek van databestanden, het zogenaamde *datamining*, aan bod. Dit is een

techniek die bijvoorbeeld in het bedrijfsleven wordt gebruikt om marktonderzoek te doen en bijvoorbeeld bij de belastingdienst om profielen te maken van fraudeurs. Hierbij kunnen door het gebruik van profielen ongewenste gevolgen zoals risicoselectie of uitsluiting ontstaan. Tevens worden in deze paragraaf aanbevelingen gedaan voor het omgaan met vervuilde bestanden of het ongewenst gebruik van persoonsgegevens.

Paragraaf 3.4 gaat in op de rol van de overheid als ontwerper van nieuwe wetgeving. Sectorale wetgeving kan gevolgen hebben voor de privacy van burgers. Het is van belang dat nieuwe wetgeving wordt getoetst aan de WBP en aan internationale richtlijnen. We kunnen immers veronderstellen dat met name bij sectorale wetgeving, sectoraal belang boven het privacybelang gaat. Ook het handhaven van de privacywetgeving zelf komt in deze paragraaf aan de orde.

De laatste paragraaf van hoofdstuk drie gaat in op de rol van de overheid als handhaver van openbare orde en veiligheid. Hierbij is het belang van de overheid tegengesteld aan de bescherming van de privacy. In de praktijk blijkt dat soms een groter belang wordt gehecht aan opsporing en vervolging dan aan privacy.

Hoofdstuk vier is concluderend van aard. In paragraaf 4.1 beantwoordt de Raad de vragen over gewenst beleid met betrekking tot ICT in relatie tot de privacy en over de verantwoordelijkheid. In de volgende paragraaf worden de kernvragen uit de adviesaanvraag nog eens herhaald en apart beantwoord. In de laatste paragraaf worden concrete aanbevelingen gedaan. De aanbevelingen komen ook in de afzonderlijke hoofdstukken aan de orde, maar worden aan het eind van het advies in onderlinge samenhang besproken.

2.
‘ICT en privacy’ in de verzorgingsstaat

2.1
Inleiding

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft zichzelf tot doel gesteld in 2002 minimaal een kwart van de publieke dienstverlening langs elektronische weg af te handelen.[17] De relatie tussen overheid en burger in de verzorgingsstaat en ‘ICT en privacy’ betreft de wisselwerking tussen het toepassen van ICT bij het uitvoeren en verbeteren van de overheidsdienstverlening en de bescherming van de persoonlijke levenssfeer van de burgers. De vraag uit de adviesaanvraag die hierbij aansluit luidt: zijn er mogelijkheden om de handelingsruimte van de overheid te vergroten – de dienstverlening te verbeteren – zonder de privacy van de burgers aan te tasten?

In het algemeen geldt dat voor het uitvoeren van overheidstaken in de dienstverlenende sfeer gegevens van burgers nodig zijn. Indien de burgers toestemming voor gegevensverwerking voor een bepaalde dienst hebben verleend, geldt volgens de Raad het volgende uitgangspunt. Gegevensverwerking door de overheid in de verzorgingsstaat dient met een zo minimaal mogelijk gebruik van persoonsgegevens te geschieden.

In dit hoofdstuk wordt rekening gehouden met sectorale belangen in relatie tot de privacybeleving. Voor een specifieke taak zoals bijvoorbeeld het verlenen van huursubsidie heeft de overheid specifieke informatie nodig, zoals het inkomen van de desbetreffende burger en de huurprijs van zijn woning. Er zijn verschillende criteria waaraan de dienstverlening moet voldoen, zodat zowel de overheidstaak kan worden uitgevoerd als de privacy van de burger kan worden gewaarborgd.

Rekening houden met de privacy van burgers betekent natuurlijk niet dat het gebruik van persoonsgegevens per definitie een bedreiging voor de privacy is. Integendeel, burgers zijn onder bepaalde voorwaarden bereid hun gegevens af te staan. De richtlijnen voor goed gebruik van gegevens in relatie tot verschillende vormen van overheidsdienstverlening worden in paragraaf 2.2 besproken. Bij het bespreken van deze criteria voor ‘goede’ gegevensverwerking wordt ook ingegaan op het wetsvoorstel Wet Bescherming Persoonsgegevens.

Een nieuwe vorm van overheidsdienstverlening is pro-actief beleid. Pro-actief beleid varieert van het gericht sturen van een aanmeldingsformulier voor een subsidie aan belanghebbenden, tot het uitvoeren van een subsidie of kwijtscheldingsregeling zonder dat de burger daarom hoeft te vragen.

---

[17] Actieprogramma Elektronische Overheid. TK 26 387, 1998-1999.

Na het bestuderen van de criteria voor goede publieke dienstverlening met inachtneming van de privacy wordt de aandacht gericht op de inrichting van de informatiehuishouding van de overheid. Hiervoor zullen in paragraaf 2.3 verschillende systemen voor informatiebeheer worden besproken. De Raad gaat in op vragen zoals: zijn landelijke registraties te prefereren boven decentrale registraties en wat is de positie van sectorale verwijsindices ten opzichte van centrale registers? Hierbij zal blijken dat veel meer dan de keuze tussen centrale of sectorale registers, het toekennen van autorisaties van belang is.

Als laatste zal, bij de bespreking van het voorstel voor elektronisch stemmen, de afweging tussen het gebruik van ICT en de mogelijke schending van de privacy in de democratie aan de orde komen.

2.2
Dienstverlening

Voor dienstverlening heeft de overheid vaak persoonsgegevens nodig om bijvoorbeeld te beoordelen of iemand recht heeft op een dienst. In algemene zin hebben burgers hiertegen geen bezwaar. Een taak van de overheid is hierbij oplettend te zijn, zodat geen ondoordacht gebruik wordt gemaakt van persoonsgegevens.

Burgers zijn onder bepaalde voorwaarden bereid hun persoonsgegevens af te staan. Vooropgesteld staat volgens de Raad de algemene norm van informatievrijheid van de burgers. Specifieke criteria voor gegevensverwerking zijn: duidelijkheid, doelbinding, transparantie en voorspelbaarheid.
In relatie tot de overheid wordt om *duidelijkheid* gevraagd. Dit betreft allereerst duidelijkheid met betrekking tot het doel van de gegevensverwerking. Pas in relatie tot het doel kan worden beoordeeld of verwerking van persoonsgegevens een privacyschending is. De nadruk op *doelbinding* sluit aan bij de bevinding dat burgers zich niet in het algemeen, maar in specifieke relaties zorgen maken over privacy. Medische gegevens afstaan bij een huisarts is minder privacygevoelig dan bij een verzekeraar. Andere voorwaarden zijn *transparantie* of helderheid. Wat is precies waarvoor nodig. *Voorspelbaarheid* is een andere factor die de burger van de overheid verlangt. Wanneer gegevensgebruik voorspelbaar is, zal de burger niet het gevoel hebben dat zijn privacy wordt geschonden. Juist het idee ‘ze doen maar wat met al mijn gegevens’ zorgt voor een onbehaaglijk gevoel. Als laatste is *zeggenschap* genoemd. Invloed en recht op verzet over het gebruik van persoonsgegevens vermindert de angst voor privacyschending. Maar hierbij merkt de Raad op dat het criterium zeggenschap direct voorvloeit uit de norm van informatievrijheid. Zeggenschap komt nader aan de orde wanneer we een bijzondere vorm van diensverlening, namelijk pro-actieve dienstverlening, bespreken.

Voor het voldoen aan alle genoemde criteria is bewustwording bij de *gebruiker* van de gegevens noodzakelijk. Meer dan wat wel of niet mag, geldt duidelijk-

heid als vereiste voor waarborg van de privacy. Hiervoor is bewustwording van ambtenaren nodig. Zij dienen niet langer gewoon gegevens door te geven, maar na te denken over de noodzaak en legitimiteit daarvan.[18]

De hierboven onderscheiden criteria komen in grote mate overeen met de vereisten voor gegevensverwerking zoals beschreven in het wetsvoorstel Wet Bescherming Persoonsgegevens (WBP).

De Europese richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van gegevens is de basis van de nieuwe WBP. De huidige Wet Persoonsregistraties (WPR) moet worden aangepast omdat de WPR niet voldoet aan de Europese richtlijn. De Europese privacyrichtlijn is opgesteld in oktober 1995 en moest drie jaar na dato (24 oktober 1998) in alle lidstaten worden geïmplementeerd. In Nederland heeft dit geleid tot het ontwerp van een nieuwe privacywet; de Wet Bescherming Persoonsgegevens. Deze is reeds behandeld en goedgekeurd in de Tweede Kamer (op 23 november 1999), maar is nog niet van kracht omdat de Eerste Kamer hierover nog moet oordelen. Op 11 januari jongstleden heeft de Europese Commissie aangekondigd Nederland voor het Europese Hof van Justitie te dagen omdat Nederland (vooralsnog) heeft verzuimd de Europese richtlijn om te zetten in wetgeving. De Europese richtlijn ziet behalve op vrij verkeer van persoonsgegevens binnen de Europese Unie, ook toe op de bescherming van persoonsgegevens en de persoonlijke levenssfeer.

De WBP[19] bevat vijf centrale artikelen die de gegevensverwerking van algemene persoonsgegevens behelzen. Het eerste – artikel 6 – bepaalt dat persoonsgegevens op *behoorlijke en zorgvuldige* wijze dienen te worden verwerkt. Artikel 7 beschrijft de *doelbinding* bij het verkrijgen en verwerken van data. Doelbinding vereist dat gegevens alleen verwerkt worden voor een van te voren gespecificeerd en gerechtvaardigd doel. Artikel 9 sluit hierbij aan, en stelt vervolgens dat gegevens niet mogen worden verwerkt op een wijze die *onverenigbaar* is met de doeleinden waarvoor ze zijn verkregen. In artikel 8 wordt een zestal gronden voor toelaatbare gegevensverwerking beschreven. Dit artikel behelst bovendien dat bij elke verwerking moet zijn voldaan aan beginselen van *proportionaliteit en subsidiariteit*. Het proportionaliteits-beginsel houdt in dat de inbreuk op de belangen van de betrokkene bij de verwerking van persoonsgegevens niet onevenredig mag zijn met het doel waarvoor de gegevens worden verwerkt. Ingevolge het subsidiariteitsbeginsel

---

[18] De Registratiekamer wijst in februari 1999 op onzorgvuldige beveiliging en tekortschieten bij geheimhoudingsverplichting bij GBA's. In: Persbericht Registratiekamer (18-02-1999) 'Beveiliging bevolkingsgegevens onvoldoende'.

[19] Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)
EK 25 892, 1999-2000.

mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, kunnen worden verwezenlijkt. Verder is de informatieplicht naar de betrokkene toe vergroot. De betrokkene moet op de hoogte worden gebracht van het gebruik en het verwerken van zijn of haar persoonsgegevens. Deze plicht vervalt echter indien het onmogelijk is of onevenredige inspanning kost de betrokkene in te lichten. Artikel 11 tenslotte, stelt dat het doel waarvoor de gegevens zijn verzameld en worden verwerkt, bepalend is voor de hoeveelheid en soort gegevens die onderwerp van verwerking vormen. De gegevens dienen toereikend, terzake dienend en niet bovenmatig te zijn. Tevens dienen persoonsgegevens juist en nauwkeurig te zijn.

Het is opmerkelijk dat de normen voor verantwoorde omgang met gegevens die zijn genoemd door de burgers aan het begin van deze paragraaf in hoge mate overeenkomen met de vereisten in de WBP.

De Raad is van mening dat gebruik van persoonsgegevens aan de betrokken burgers dient te worden gevraagd, maar erkent dat in sommige gevallen – zoals bij het belastingvoorbeeld – het gebruik van persoonsgegevens eenvoudigweg een verplichting betreft. Uit bovenstaande beschrijving van voorwaarden van burgers en artikelen uit de WBP blijkt dat de overheid in principe gegevens van burgers mag gebruiken, zolang de burger maar weet hoe en waarom en hierover zeggenschap heeft.

Welke instrumenten kunnen worden ingezet om deze situatie, namelijk ‘zolang de burger maar weet hoe en waarom’ te bereiken? Simpelweg zeggen dat de WBP gevolgd zal worden, helpt niet omdat privacybeleving specifieke relaties betreft, en omdat de meeste burgers, de slogan ‘iedere burger dient de wet te kennen’ ten spijt, de wet niet kennen. Een taak van de overheid is de regels die voortvloeien uit de WBP in gewoon, begrijpbaar, niet-juridisch Nederlands te vertalen en deze regels kenbaar te maken aan haar burgers. Er zijn reeds voorlichtingsplannen in ontwikkeling. De Raad ondersteunt deze plannen. Met behulp van overheidsvoorlichting – bijvoorbeeld via folders in postkantoren maar ook door Postbus 51-spotjes – moet bekendheid worden gegeven aan de WBP. Hierbij geldt dat het geven van voorlichting een gangbare procedure is nadat een nieuwe wet van kracht is geworden.

Algemene voorlichting over de WBP is slechts een begin en bovendien een momentopname. Juist in specifieke relaties met de burger, pleit de Raad voor reguliere voorlichtingsactiviteiten. Een beleidsinstrument als het geven van voorlichting kan het gevoel van privacybescherming doen toenemen. Een sociale dienst van een gemeente kan bijvoorbeeld aan zijn cliënten uitleggen waarom welke gegevens voor de dienstverlening nodig zijn. Hiermee wordt de transparantie vergroot en indien aanwezig wordt de beleving van privacy-schending verkleind of geheel weggenomen. Het geven van voorlichting is een instrument dat de overheid kan inzetten om voorwaarden voor burgers te

scheppen voor omgang met 'ICT en privacy'. Door het geven van gerichte voorlichting kan de handelingsruimte van de overheid gelijk blijven of zelfs worden vergroot, zonder dat de privacy van de burgers wordt geschonden.

Proportionaliteit en de eis dat de gegevens terzake dienend en niet bovenmatig zijn, vereist een gedragsverandering bij de uitvoerende ambtenaren. Hierbij dient de overheid zichzelf regels op te leggen, zoals het niet meer gegevens vragen dan nodig is voor het betreffende doel. Proportioneel gegevensgebruik vereist dat de verwerking van gegevens in verhouding is met het doel van de gegevensverwerking. Met andere woorden: voor een relatief onbelangrijke dienst zal een burger geen gevoelige persoonsgegevens willen afstaan. Ambtenaren moeten met dit beleid nog leren omgaan en zullen bovendien ook meer aandacht moeten gaan schenken aan zorgvuldig gegevensbeheer. Voorbeelden van onbeveiligde GBA's en onzorgvuldige omgang met wachtwoorden op afdelingen waar gegevens verwerkt worden, zijn nog geen uitzondering. Uit een onderzoek bij de Belastingdienst is gebleken dat medewerkers die inzage hebben in gevoelige informatie regelmatig beveiligingsregels overtreden: 71% verlaat wel eens de werkplek zonder beveiliging van de computer, 52% bergt niet altijd aan het eind van de dag de dossiers op in een afgesloten kast, 36% maakt wel eens gebruik van het wachtwoord van een collega en 27% raadpleegt wel eens onbevoegd bestanden.[20]

Een belangrijk instrument ter bescherming van de informationele privacy – dat ook in de volgende paragraaf aan de orde zal komen – is het niet doorgeven van gegevens, maar het laten uitzoeken wie aan bepaalde criteria voldoen. Dit wordt 'ontkoppeld koppelen' genoemd. Bijvoorbeeld voor het kwijtschelden van een gemeentelijke heffing is een bestand met namen en adressen nodig van mensen die een inkomen hebben onder een bepaald minimumbedrag. De inkomensgegevens zelf hoeven niet bij de betreffende afdeling aanwezig te zijn. De belastingdienst kan aangeven welke personen onder dit minimumbedrag vallen zonder de inkomensgegevens daadwerkelijk af te staan.
In het kader van fraudebestrijding bij sociale diensten worden ook gegevens gekoppeld met onder andere de belastingdienst. Hiermee kan worden gecontroleerd of de betreffende burger niet heeft gewerkt ten tijde van zijn of haar bijstandsuitkering. In plaats van complete *datafiles* aan elkaar te koppelen zou door ontkoppeld te koppelen een lijstje met namen van bijstandsontvangers die hebben gewerkt, voldoende zijn.

Een aanbeveling van de Raad is het periodiek – bijvoorbeeld jaarlijks – verstrekken van een data-overzicht, waarbij iedere burger alle over hem of haar bekende informatie opgestuurd krijgt, omdat dit de privacybeleving van burgers kan laten toenemen. Hiermee komt de overheid zowel tegemoet aan de wens voor meer transparantie als aan zorgvuldigheid omdat burgers de over

[20] Staatscourant, 11-11-1999.

hen bekende gegevens op juistheid kunnen toetsen.

Zoals in de inleiding van dit advies reeds is aangekondigd, is de wisselwerking tussen 'ICT en privacy' in de verzorgingsstaat met name aan de orde bij pro-actieve dienstverlening. Dienstverlening door de overheid wordt pro-actief genoemd indien de overheid reeds bekende informatie gebruikt – lees het koppelen van bestanden – voor het actief en gericht verlenen van diensten aan de burger.[21] ICT is een strategisch instrument dat kan worden ingezet om de dienstverlening te verbeteren. Pro-actieve dienstverlening is echter geen logisch gevolg van ICT. Dit wordt soms verondersteld omdat het gebruik van ICT – bijvoorbeeld door het koppelen van bestanden en aanbieden van digitale overheidsinformatie – pro-actieve diensverlening mogelijk maakt. Echter, de keuze om gericht en actief diensten te verlenen, in plaats van bijvoorbeeld reactief of responsief, en dus de vraag naar de wenselijkheid van pro-actief beleid, is onafhankelijk van techniek en is een bestuurlijk vraagstuk.

Pro-actieve dienstverlening door de overheid vergroot de doeltreffendheid en de doelmatigheid van het openbaar bestuur.[22] In de eerste plaats omdat de kwaliteit van de dienstverlening zal verbeteren. Pro-actieve dienstverlening betekent meer 'gemak' voor de burger, bijvoorbeeld doordat burgers gericht geïnformeerd worden over hun rechten. Tegelijkertijd kan worden verondersteld dat de overheid door pro-actieve dienstverlening tot een doelmatigere bedrijfsvoering zal komen. Het automatisch uitvoeren van regelingen zal de bureaucratie van de uitvoeringsorganisaties verkleinen. Pro-actieve dienstverlening zorgt ook voor een vergroting van de effectiviteit van de overheid. Hiermee wordt bedoeld dat door pro-actief optreden het niet-gebruik van overheidsvoorzieningen kan worden tegengegaan.[23]

Dienstverlening volgt het patroon van automatisch uitvoeren wanneer de dienst voor de burger belastende – lees verplichte – regelingen betreft of wanneer het een regel in het 'algemeen belang' betreft. Dit zijn tegelijkertijd de diensten waarbij informatievrijheid of informatie-eigendom van burgers niet helemaal opgaat, omdat een deel van deze diensten 'verplichtingen' van de burgers betreft. Natuurlijk dient de overheid ook in deze gevallen zorgvuldig met persoonsgegevens om te gaan en blijft minimalistisch gegevensbeheer het credo. Een voorbeeld is dat bij de overheid bekende informatie wordt gebruikt om belastingaanslagen te versturen.
De gemeentelijke basisadministratie wordt ook gebruikt voor pro-actief beleid. Voorbeelden van pro-actief beleid op basis van de GBA zijn het verstrekken

---

[21] BZK, 1999, Voorbij het loket.

[22] BZK, 1999, Bewegingen in het bestuur.

[23] Dat dit relevant is blijkt onder meer uit de SCP armoedemonitor van 1997; het volledig dan wel partieel niet-gebruik van de individuele huursubsidie bedroeg in 93/94 zo'n 53% van de totale doelgroep.

van kinderbijslag, de Ent-administratie, de Wet op de Orgaandonatie en de Oproepingskaart voor het stemmen. Deze voorbeelden betreffen het automatisch uitvoeren van diensten op basis van geboorte en leeftijd. Het onderscheid tussen deze voorbeelden en het toekennen van subsidies of kwijtscheldingen is dat eerstgenoemde in het algemeen belang zijn, terwijl laatstgenoemde het financieel belang van individuele burgers kunnen dienen. Bij de meeste regelingen waarbij automatisch uitvoeren als vorm van pro-actieve dienstverlening wordt toegepast, blijft de privacy voldoende beschermd. Het belang van deze regelingen staat niet ter discussie en voor deze regelingen worden geen gevoelige persoonsgegevens gebruikt. Of anders gezegd: het betreft ook niet de terreinen waarvan burgers aangeven dat het privacygevoelige beleidsterreinen zijn.

In het kader van armoedebestrijding wordt ICT ingezet om pro-actief diensten te verlenen waarbij het belang van de burger voorop staat. Het niet-gebruik van individuele huursubsidie wordt teruggedrongen als woningbouwverenigingen, belastingdienst en gemeentelijke sociale diensten bestanden koppelen. Voor een viertal inkomensafhankelijke maatregelen in het kader van armoede bestijding zijn pilot-projecten gestart. Hierbij wordt pro-actieve dienstverlening aangeboden voor individuele huursubsidie, bijzondere bijstand, kwijtschelding gemeentelijke heffingen zoals onroerendzaakbelasting, afvalstoffenheffingen en waterschapsbelasting, en gemeentelijke reductieregelingen. Koppelingen van bestanden bijvoorbeeld van belastingdienst, sociale dienst en gemeenten zijn veelal ontwikkeld in het kader van fraudebestrijding. Deze koppelingen worden, door ze ook te gebruiken voor armoedebestrijding, nu ook in het financiële belang van de burger toegepast. De reacties op pro-actieve armoedebestrijding bij de gemeenten in de *pilotprojecten* zijn positief. Gemeenten gebruiken verschillende niveaus van pro-actieve dienstverlening – variërend van het versturen van een aanvraagformulier, huisbezoeken, tot automatische prolongatie – voor armoedebestrijding.

Bij de vormen van pro-actieve dienstverlening waarbij gebruik wordt gemaakt van het koppelen van bestanden en het selecteren op basis van inkomensgegevens, wordt door de overheid ‘voor ons gedacht’, worden ‘bestanden gekoppeld’, en kan dus een inbreuk worden gemaakt op de privacy. De vraag of ‘een burger niet discreet in armoede mag leven’ is in het kader van de privacy een legitieme vraag. Juist dit gevoel kan een inbreuk vormen op de persoonlijke levenssfeer. De angst voor een alles registrerende overheid en voor paternalisme kan volgens de Raad worden weggenomen door een gedifferentieerd systeem voor pro-actieve dienstverlening. Hierbij kan een burger zelf aangeven waarvoor hij wel of niet in aanmerking wil komen. Dit is in overeenstemming met het principe van informatievrijheid en dient een vanzelfsprekende gang van zaken te worden in gevallen waarbij ‘het ontvangen van dienstverlening geen verplichting vormt’. Deze methode heeft een wettelijke grondslag in de WBP, zie het recht op verzet, en wordt ook door de

Raad aanbevolen in de private sector wanneer het gaat om het ontvangen van *direct-mail*, reclame-folders en telefonische marketinggesprekken. De overheid dient hiervoor de voorwaarden te scheppen en dient dus de burger de keuzevrijheid voor te leggen en ervoor te zorgen dat de burger genoeg informatie over zijn rechten en plichten heeft om zelf een keuze te kunnen maken. Tevens geldt ook voor deze diensten in het kader van armoedebestijding, dat wanneer ze door de burger worden geaccepteerd een minimalistisch gegevensbeheer het credo is. De Raad wijst erop dat burgers attent kunnen worden gemaakt op een dienst en een keuzemogelijkheid kunnen krijgen, zonder dat daarvoor gegevens daadwerkelijk van de ene organisatie naar de andere organisatie behoeven te gaan.

Concluderend geldt dus dat de overheid op een verantwoorde wijze met gegevensverwerking moet omgaan. Hierbij is informatievrijheid van de burger het uitgangspunt en is een zo minimaal mogelijke gegevensverwerking een belangrijk instrument van de overheid om aan de wensen van de burgers te voldoen. Het onderscheid tussen regels en diensten met een bindend en een vrijwillig karakter dient invloed te hebben op de gegevensverwerking. Hierbij dient de informatievrijheid van burgers bij diensten met een vrijwillig karakter altijd te worden gerespecteerd. Om dit te bereiken zal actief moeten worden gewerkt aan bewustwording bij de overheid zelf. Aan de vereisten voor een verantwoorde omgang met gegevens, zoals genoemd door de burgers en beschreven in de WBP, namelijk proportionaliteit, doelbinding, transparantie en voorspelbaarheid moet worden voldaan. Zowel een cultuurverandering bij de overheid, als het inzetten van minimalistisch gegevensbeheer, ontkoppeld koppelen, het verstrekken van gegevensoverzichten, het geven van voorlichting, en het creëren van een gedifferentieerd systeem voor pro-actieve dienstverlening, zijn noodzakelijk.

2.3
Informatiehuishouding van de overheid

In deze paragraaf wordt een kort overzicht gegeven van een aantal belangrijke informatiebestanden van burgers, de Gemeentelijke Basisadministratie en de bestanden voor de sociale zekerheid; het zogenaamde Cliënt-Volg-Communicatie-Stelsel (CVCS) en de Inlichtingenbank (IB). Vervolgens wordt een korte beschrijving van de Belgische Kruispuntbank Sociale Zekerheid gegeven, omdat dit systeem goed functioneert en mogelijk voor Nederland als voorbeeld kan dienen. Hierna volgt een korte beschrijving van het programma, opgezet door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, ‘stroomlijning basisgegevens’.
Vervolgens wordt ingegaan op de positie van centrale- ten opzichte van decentrale basisregistraties, op het verschil tussen sectorale verwijsindexen ten opzichte van centrale registers en op het gebruik van intersectorale persoonsnummers en identificatie met behulp van biometrie. Als laatste zal in deze sectie een aanbeveling worden gedaan voor het houden van een *privacy-audit* bij overheidsinstellingen.

Voor een uitgebreide beschrijving van de rol van informatietechnologie voor verbetering van de dienstverlening en in het bijzonder de inrichting van de informatiehuishouding wordt verwezen naar het preadvies over dit onderwerp uitgebracht door de Raad voor het openbaar bestuur.[24] In dit preadvies is reeds geconcludeerd dat er mogelijkheden zijn voor verregaande samenwerking, zonder verlies van de eigen identiteit.

2.3.1
De GBA en informatiebestanden in de sociale zekerheid

De *gemeentelijke basisadministratie* is een geautomatiseerde bevolkingsadministratie. De GBA bestaat uit een authentieke bron van basisgegevens die decentraal op gemeentelijke niveau worden opgeslagen en beheerd. In de GBA zijn de volgende registers te vinden: geboorteregister, bevolkingsregister, trouwregister, leerplichtigenregister, (dienstplichtigenregister) en kiesregister. De volgende regels worden door het GBA-stelsel nageleefd:

- persoonsgegevens worden decentraal verzameld, vastgelegd en beheerd;
- persoonsgegevens dienen enkelvoudig te worden verzameld;
- persoonsgegevens worden zo mogelijk multifunctioneel gebruikt;
- standaard verstrekkingen van persoonsgegevens dienen op basis van een wet plaats te vinden.[25]

Het enkelvoudig verzamelen en multifunctioneel gebruik is, mits goed geregeld, in het belang van de burger omdat hij daardoor niet vaker dan nodig gegevens hoeft door te geven. De verwijsindex in de GBA, die slechts door een beperkt aantal overheidsinstellingen mag worden gebruikt, geeft aan in welk register welke informatie te vinden is. Dit systeem kan op allerlei beleidsterreinen worden ingevoerd.

Het project CVCS is een onderdeel van de ontwikkeling bekend staande onder de naam Samenwerking Werk en Inkomen. Sociale diensten, uitvoeringsinstellingen en arbeidsbureaus gaan samenwerken om uitkeringsgerechtigden aan het werk te helpen. Hiervoor worden de Centra voor Werk en Inkomen opgericht met als voordeel voor de cliënt dat hij of zij nog maar naar één loket hoeft te gaan. Het CVCS moet mogelijk maken dat betrokken organisaties burgers kunnen volgen in het proces om weer aan het werk te komen. Het CVCS betreft dus het gebruik van informatietechnologie in de sociale zekerheid. Het CVCS is van start gegaan met een zevental praktijkproeven. Bij deze *pilots* heeft de technische haalbaarheid van het CVCS-Stelsel zich volgens minister De Vries van Sociale Zaken en Werkgelegenheid bewezen, maar het gebruik van het CVCS is nog beperkt.[26]
Het CVCS is geen geïntegreerd systeem dat bestaande informatiesystemen

---

[24] Zuurmond, 1998.

[25] Mutsaers, 1998.

[26] Minister De Vries, 26 november 1999.

vervangt. Voor de sector arbeid en inkomen worden alle gegevens gestroomlijnd en gestandaardiseerd en het CVCS is een voorziening die communicatie tussen de verschillende partijen regelt.

Van Eck stelt overigens in *Privacy en Informatie* van oktober 1999 dat in de Centra voor Werk en Inkomen, waar nog geen gebruik wordt gemaakt van CVCS, in sommige gevallen als tussenoplossing is gekozen voor rechtstreekse toegang van elkaars databases.[27] Dit is in het kader van privacybescherming geen wenselijke praktijk. Zeker wanneer een der partijen zich niet alleen op de publieke, maar ook op de marktsector richt.

Inmiddels is ook het Inlichtingenbureau (IB) van start gegaan. Dit bureau voert voor de sociale diensten gegevensuitwisseling uit met andere instanties. Als de sociale dienst informatie nodig heeft kan zij met een verbinding naar het IB volstaan. Het inlichtingenbureau is ontwikkeld om voor de sociale diensten gegevens op fraude te controleren. In 1998 is een vijftal *pilots* van start gegaan in Hellevoetsluis, Deurne, Nijmegen, Arnhem en Apeldoorn. In het IB worden onder andere gegevens uitgewisseld tussen sociale diensten, de studiefinanciering en de uitvoerders van de werknemersverzekeringen.

Voor uitvoering van deze *pilots* (zowel CVCS en IB) is gebruikgemaakt van het RINIS-(Routerings-Instituut (inter)Nationale Informatie Stromen)netwerk. Aangesloten bij het RINIS-netwerk zijn de sociale diensten, de studiefinanciering, de gemeenten (via de GBA), de Sociale Verzekeringsbanken, de Belastingdiensten, het ministerie van Justitie en de uitvoerders van de werknemersverzekeringen. Dit netwerk regelt het berichtenverkeer tussen verschillende instanties en verschillende sectoren. Iedere sector ontwikkelt een eigen Sectoraal Aanspreekpunt (SAP), het zogenaamde elektronische postkantoor, en het gegevensverkeer tussen uitvoerders in verschillende sectoren verloopt via de sectorloketten. Een sector heeft een eigen SAP en een centrale gemeenschappelijke opslag- en raadpleegindex met behulp waarvan gegevens kunnen worden doorgestuurd. In de instanties binnen het CVCS, dus instanties gelieerd aan de sociale zekerheid, is deze gemeenschappelijke index het sofi-nummer.

Zowel het CVCS als het IB zorgen voor communicatie tussen verschillende instanties en gaan dus uit van het concept van een basisregistratie tezamen met sectorale verwijzingen. Een voordeel van deze systemen ten opzichte van andere is dat gegevens maar één keer worden opgeslagen en via de verwijsindexen – na autorisatie – toch met elkaar kunnen worden verbonden.

---

[27] Eck Van, 1999.

2.3.2
Kruispuntbank

Het RINIS-netwerk is vergelijkbaar met de Belgische Kruispuntbank, het elektronische netwerk voor de Belgische sociale zekerheid. De Kruispuntbank is een sectorbreed elektronisch netwerk voor gegevensuitwisseling. Een centrale gegevensbank achtte men niet wenselijk wegens onderhoudsproblemen en mogelijke problemen met beveiliging en privacy. Daarom is een decentraal netwerk opgezet. De Kruispuntbank verwijst instanties die recht hebben op bepaalde informatie via codes naar de vindplaats van gegevens. In dit systeem blijven gegevens decentraal opgeslagen en kunnen gegevens van andere instellingen pas na autorisatie worden geraadpleegd. Ook is wettelijk vastgelegd dat gegevens van burgers niet meer dan één keer mogen worden gevraagd. De Kruispuntbank fungeert ook als een soort vertaalbureau. Dit was zeker in de beginfase van groot belang omdat niet alle instanties dezelfde computertaal of software gebruikten.

De Kruispuntbank is een grote verbetering voor de burger bijvoorbeeld als het gaat om de relatie tussen Ziekenfonds en verzekerde en voor pro-actieve kwijtschelding van belastingen. Hierbij hoeft de gemeente niet om inkomensgegevens te vragen, maar stuurt de gemeente een groslijst met al haar burgers tezamen met voorwaarden om in aanmerking te komen voor vrijstellingen, naar de Kruispuntbank. Deze checkt welke burgers voor een vrijstelling in aanmerking komen en verwijdert hen van de groslijst. De bewerkte lijst gaat terug naar de gemeente zodat de gemeente de burgers die in aanmerking komen voor een vrijstelling niet behoeft aan te schrijven. De gemeente kan dan zien wie niet behoeft te betalen, maar heeft geen beschikking over inkomensgegevens. De Belgische situatie toont aan dat ICT niet alleen geschikt is voor fraudebestrijding, maar ook voor verbetering van dienstverlening aan de burger. Tegelijkertijd wordt hierbij, door gebruik te maken van ontkoppeld koppelen, rekening gehouden met de privacy van de burgers.

2.3.3
Programma stroomlijning van basisgegevens

In het Actieprogramma Elektronische Overheid bevindt zich een programmaonderdeel gericht op het opzetten van authentieke basisregistraties, onder de noemer ‘stroomlijning van basisgegevens’.[28] Hierbij staat het opzetten van authentieke registraties, vergelijkbaar met de GBA voor persoonsgegevens, centraal. In deze registraties, die de vorm hebben van registraties met sectorale verwijsindexen, wordt uitgegaan van de principes van het slechts éénmalig en op één plaats vastleggen van gegevens en wordt een verwijsindex gebruikt voor koppelingen tussen bestanden. Dit programma betreft voorstellen voor het opzetten van nieuwe- en certificeren van bestaande sectorale authentieke registraties op bijvoorbeeld terreinen als ‘personen’ (GBA), ‘bedrijven’ (Basis

[28] Actieprogramma Elektronische Overheid. TK 26 387, 1998-1999.

Bedrijven Register) en ‘inkomen’. De doelstellingen zijn vergelijkbaar met de doelstellingen van systemen als de GBA of het CVCS, namelijk verbetering van de efficiency van de overheid, transparantie, één-loket-gedachte, fraudebestrijding (zie het IB) en armoedebestijding (zie pro-actieve dienstverlening). Het doel van dit veelomvattende programma is het oprichten van een goede basisinfrastructuur. De vraag wie geautoriseerd wordt om in een registratie te kijken, wordt overgelaten aan de politiek. Hiervoor zijn onder meer de beperkende bepalingen van de WBP van kracht.

2.3.4
Methoden voor gegevensuitwisseling beschouwd

Om te bepalen hoe de informatiehuishouding van de overheid eruit zou moeten zien is het raadzaam de verschillende methoden voor elektronische gegevensuitwisseling op een rij te zetten. Het is in het kader van dienstverlening of fraudedetectie soms nodig gegevens uit verschillende basisregistraties te ‘koppelen’. Dit koppelen kan gebeuren door:

- erin te kijken (hierbij dient te worden opgemerkt dat dit ook bepaalde delen van een bestand kan betreffen), of
- daadwerkelijk bestanden te koppelen, of
- gegevens bij elkaar te controleren. Dit laatste is het zogenaamde ontkoppeld koppelen. Deze optie verdient vanuit privacy-oogpunt de voorkeur.

De registraties binnen het CVCS en het IB zijn decentrale basisregistraties die via sectorale verwijsindexen – het CVCS en het IB – gekoppeld kunnen worden.[29] Bij het CVCS en het IB weet men wie welke gegevens uit de basisregistraties mag opvragen en waar deze gegevens te vinden zijn. In ons voorbeeld is RINIS het netwerk dat dit mogelijk maakt. Maar deze stap kan ook door het sectorale aanspreekpunt worden gedaan. Met deze verandering zou het Nederlandse stelsel erg dichtbij de Belgische Kruispuntbank komen.

Een verschil tussen het CVCS en bijvoorbeeld de Kruispuntbank is het aantal organisaties en de reikwijdte van de organisaties binnen het netwerk. Binnen het CVCS zitten alleen organisaties waarvan we kunnen zeggen dat ze tot de sector Werk en Inkomen behoren. In de Kruispuntbank bevinden zich behalve organisaties uit die sector, ook organisaties en dus registraties uit de gezondheidszorg. De Kruispuntbank wordt een sectorale verwijsindex genoemd, maar kan eigenlijk worden beschouwd als een boven-sectorale verwijsindex waarin alle vormen van sociale zekerheid zijn opgenomen.

Wat de nieuwste ontwikkelingen in Nederland en de Kruispuntbank in België met elkaar gemeen hebben, is dat de registraties ‘blijven waar ze zijn’, ‘dat ze maar éénmaal worden vastgelegd’ en dat een ‘derde actor’ zorgt voor de

---

[29] Binnen het IB bevindt zich ook een centrale basisregistratie, namelijk de studiefinanciering.

uitwisseling van gegevens. De Raad acht de trend gegevens niet meer dan een keer op te slaan, vergelijkbaar met de Wet Eenmalige Gegevensaanlevering die in België van kracht is, een goede ontwikkeling. Het maximaal eenmaal opslaan is goed voor de transparantie van de informatiehuishouding. Hierbij dient ook aan de burger kenbaar te worden gemaakt welke gegevens kunnen worden gekoppeld en wie voor gebruik van welke gegevens geautoriseerd is.

2.3.5
Sectorale verwijsindices versus centrale registers
De vraag over informatiehuishouding uit de adviesaanvraag richt zich met name op het onderscheid tussen sectorale verwijsindices en centrale registers. Het verschil tussen beide is als volgt te omschrijven: bij de sectorale verwijsindices blijven de gegevens in de basisregistraties, terwijl bij een centraal register de gegevens naar dit register worden verplaatst. Dit lijkt een helder onderscheid, maar het is in het kader van digitalisering van informatie niet zo helder. De sectorale verwijsindex kan immers – indien autorisatie is verleend – gegevens uit alle basisregistraties doorgeven. Dit laatste kan ook door een centraal register worden gedaan. Alleen wanneer we over opslag van gegevens en niet over verwerking van deze gegevens spreken, is bovengenoemd onderscheid betekenisvol.

In dit advies richten wij ons echter op de gehele keten van verwerking van gegevens. Hierbij geldt dat autorisatie het sleutelwoord is. Als alleen de gegevens waar een organisatie voor het uitvoeren van een taak recht op heeft naar deze organisatie gaan, of dit nu is door middel van het beantwoorden van vragen – ontkoppeld koppelen – of door middel van het daadwerkelijk koppelen van deze gegevens, dan maakt het in feite geen verschil of de sectorbank deze gegevens voor ons koppelt of ze voor ons uit zijn ‘centraal register’ haalt. Het is echter wel van belang dat indien een centraal register wordt gevormd, dit register niet zomaar beschikbaar is voor alle organisaties in de sector. De Raad is dus van mening dat het onderscheid sectoraal of centraal niet zinvol is en benadrukt nogmaals dat minimalistisch gegevensbeheer het sleutelbegrip voor informatie-uitwisseling vormt.

2.3.6
Ontkoppeld koppelen
In veel gevallen krijgt ontkoppeld koppelen door de Raad de voorkeur boven het koppelen van gegevens, omdat bij ontkoppeld koppelen niet meer gegevens dan noodzakelijk worden verwerkt. Bij ontkoppeld koppelen gaan immers geen gegevensbestanden van A naar B, maar wordt volstaan met het antwoord op een gestelde vraag, en gaat alleen het antwoord van A naar B. In enkele gevallen, waarbij van alle betrokkenen in een gegevensbestand bepaalde gegevens nodig zijn, kan het wenselijk zijn – indien aan de privacynormen is voldaan – een deel van een bestand voor een andere organisatie via een sectorpoort te ontsluiten.

2.3.7
Landelijke versus decentrale registraties

Zoals reeds is geconstateerd, ligt in dit advies de nadruk op de verwerking van data en minder op de opslag daarvan. Vanuit het oogpunt van privacy maakt het in principe niet uit of de overheidshuishouding vanuit een centrale landelijke opslag van gegevens of vanuit decentrale opslag met verwijsindices plaatsvindt. De reden hiervoor is dat voor beide mogelijkheden (centraal of decentraal) nauwkeurig dient te worden omschreven wie, wanneer (autorisatie) en waarom, welke gegevens mag gebruiken. Echter, de kans dat er iets misgaat en de risico's wanneer er iets misgaat – bijvoorbeeld in het kader van onderhoudsproblemen en beveiliging – zijn bij een decentrale databank kleiner dan bij een centrale databank. Anderzijds vormen decentrale registraties meer potentiële bronnen waar iets mis kan gaan.

Voorts dient te worden opgemerkt dat door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoek wordt verricht naar de haalbaarheid en wenselijkheid van een centraal in plaats van een decentraal GBA. Bij dit onderzoek dient ook rekening te worden gehouden met het gegeven dat de infrastructuur – het systeem – van de GBA goed functioneert. Problemen met betrekking tot onzorgvuldigheid liggen bij de uitvoering van beleid. Een argument om de GBA-registratie decentraal te houden, is dat – voor wie autorisatie heeft – koppelen van gegevens toch mogelijk is en dat een nieuw centraal systeem opzetten veel geld en moeite kost. De ontwikkelingen bij het opzetten van informatiesystemen lijken in de richting van landelijke registers te gaan. De Raad benadrukt nogmaals dat hij een goede beveiliging en een verantwoorde methode voor het uitwisselen van gegevens van groter belang acht, dan de vorm van de dataregistratie.

2.3.8
Intersectoraal persoonsnummer en unieke persoonsidentificatie

Een ander voorstel dan de sectorale verwijsindices of de centrale – per sector – registratie is een ontwerp dat dit niveau overstijgt. Het vergroten van de handelingsruimte van de overheid kan ook tot stand komen door het koppelen van gegevens via het invoeren van een elektronische chipcard op basis van een intersectoraal persoonsnummer. Hierbij is impliciet de verwachting dat een intersectoraal persoonsnummer ook leidt tot intersectorale registraties. Dit laatste hoeft natuurlijk niet het geval te zijn. Een landelijk persoonsnummer leidt niet per definitie tot landelijke sectoroverstijgende bestanden, maar zal dit in de praktijk wel stimuleren.

Een onderscheid dient te worden gemaakt tussen intersectorale landelijke persoonsnummers (bijvoorbeeld met een elektronische chipkaart op basis van het sofi-nummer) en landelijke registraties op basis van biometrische gegevens

(bijvoorbeeld een chipkaart met vingerafdruklezer).[30]
Beide vormen van centrale registraties zijn denkbaar. De ontwikkeling van registratie met behulp van biometrie – bijvoorbeeld met het oog op een goed beveiligd paspoort of voor de overheidsidentificatiekaart – is gaande. Er is echter nog onvoldoende zekerheid over de betrouwbaarheid van deze identificatievormen. Uit proeven met biometrische herkenning blijkt dat de betrouwbaarheid op basis van een irisscan groter is dan op basis van bijvoorbeeld vingerafdrukken. Vingerafdrukherkenning, bijvoorbeeld, kan relatief eenvoudig worden gekraakt. *Hackers* – mensen die inbreken in computers om de feilbaarheid van de technologie en informatiesystemen aan te tonen – hebben op een *hackers*congres laten zien dat door het kopiëren van een vingerafdruk een herkenning kan worden vervalst.[31] 'De machine ziet het verschil niet'.

Intersectorale persoonsnummers zijn vooralsnog niet in gebruik. De Registratiekamer adviseerde bij voorstellen voor invoering van intersectorale persoonsnummers negatief.[32] De Registratiekamer gaf hierbij aan dat op uitvoeringsniveau vaak nog niet zorgvuldig genoeg wordt omgegaan met persoonsgegevens. Het sofi-nummer mocht volgens de Registratiekamer bijvoorbeeld niet als identificatie in het onderwijs worden gebruikt omdat daarmee het doelgebonden gebruik van het sofi-nummer op de helling wordt gezet. Maar of het gebruik van algemene intersectorale persoonsnummers nog lang op zich laat wachten, en in dit kader ook of het gebruik van het sofi-nummer als intersectoraal persoonsnummer nog lang op zich laat wachten, valt te bezien.

Het gebruik van één centraal persoonsnummer kan bijdragen aan efficiënt gegevensbeheer. De Raad is van mening dat ook sectorale opslag en verwerking van gegevens al kan bijdragen tot een verhoogde efficiëntie en een vergrote handelingsruimte van de overheid. Er dient bij het ontwikkelen van centrale registraties wel rekening te worden gehouden met weerstand van burgers tegen het beeld van allesomvattende registraties. Zeker gezien het gegeven dat ook bij decentrale en sectorale registraties, wanneer autorisatie is verleend, gegevens kunnen worden doorgestuurd, is de vraag of landelijke en bovensectorale registraties nodig zijn, niet onbeduidend. Praktisch gezien is de vraag die rest of een intersectorale landelijke registratie op basis van één persoonsnummer meer vertrouwen geeft door de transparantie van dat systeem,

---

[30] Biometrie is het met behulp van een meetbaar fysiek of persoonlijk kenmerk vaststellen van iemands identiteit.

[31] Stol, et al., 1999.

[32] De Registratiekamer zal na de invoering van de WBP van naam veranderen en College Bescherming Persoonsgegevens gaan heten. Deze naam past beter bij de taken omdat het College niet alleen toeziet op registratie maar op de hele keten van verwerking van persoonsgegevens.

of dat verschillende sectorale registraties met verschillende nummers meer vertrouwen geven omdat hierbij de burger niet het 'gevoel' heeft dat alles centraal is opgeslagen.
De Raad acht een ontwikkeling naar intersectorale persoonsnummers en registraties en (impliciet) daaraan gekoppeld landelijke databanken zeer waarschijnlijk, maar wijst op het grote belang van zorgvuldigheids- en privacyeisen. Bij het invoeren van centrale registratie op basis van een persoonsnummer dient autorisatie goed te worden geregeld. Hetzelfde geldt voor biometrische systemen maar daarbij moet ook nog belang worden gehecht aan betrouwbaarheid. De betrouwbaarheid van identificatie op basis van biometrie is wellicht vele malen groter dan van andere identificatiesystemen, maar juist omdat van biometrische herkenning – misschien ten onrechte – wordt verondersteld dat deze 100% waterdicht is, is voorzichtigheid geboden. Meer dan de vraag of centrale registratie de voorkeur verdient boven sectorale registratie vindt de Raad het zorgvuldig toekennen van autorisaties van belang. Voor het toekennen van autorisaties dienen alle beperkingen van de WBP in acht te worden genomen en dient een onderscheid te worden gemaakt tussen voor de burger verplichte diensten – zoals belasting betalen – en niet verplichte begunstigende diensten.

2.3.9
Audit

De uitspraken van de Registratiekamer over onzorgvuldige omgang met persoonsgegevens op uitvoeringsniveau tezamen met resultaten van een onderzoek in opdracht van het 'Radio 1-Journaal' geven aanleiding tot bezorgdheid over privacy.[33] Het onderzoek waarbij journalisten bij gemeenten om persoonlijke gegevens vroegen, leidde in de helft van de gevallen (drie van de zes) tot 'succes'. De Registratiekamer heeft onderzoek verricht naar de kwaliteit van de gemeentelijke basisregistraties en voorstellen voor een landelijke *privacy-audit* van de GBA gegevens uitgewerkt.

Als aanvulling hierop is de Raad van mening dat het zeer zinvol is een grootschalige *privacy-audit*, die een grotere reikwijdte heeft dan de GBA's, te organiseren. Een grotere reikwijdte is van belang omdat 'slordigheid' niet alleen bij de GBA's, maar bijvoorbeeld ook bij de belastingdienst, is aangetoond. Een grootschalige *audit* kan zowel bijdrage tot bewustwording van overheidsinstanties als tot daadwerkelijke privacybescherming. Hierbij wordt gedacht aan het elektronisch op elkaar afstemmen van alle overheidsgegevensbanken, het bestuderen en waar nodig aanpassen van de infrastructuur en de werking van de informatiesystemen, en het toetsen en waar nodig aanpassen van de beveiliging van de persoonsgegevens. Het invoeren van *Privacy Enhancing Technologies* (PET) ter beveiliging van gegevens, samen met strenge autorisatieregels, kan voor dit laatste, een richtlijn zijn. Een dergelijke

---

[33] Zie 'Gemeente en privacy (I & II)', In: Handboek Privacy van 5 maart 1999.

audit is een omvangrijke taak die een grootschalige aanpak vereist en wellicht het best vergeleken kan worden met het oplossen van het millenniumprobleem.

2.4
Elektronisch stemmen

In deze paragraaf wordt gekeken naar de wisselwerking tussen het gebruik van ICT en de invloed op de privacy van de burgers in een democratie. De aandacht zal worden gericht op een modieuze ontwikkeling, namelijk het locatie-onafhankelijk elektronisch stemmen.

Voor de beschrijving van de mogelijkheden en onmogelijkheden van elektronisch stemmen is mede gebruikgemaakt van informatie verkregen op de Expertmeeting *Lokatie-onafhankelijk elektronisch stemmen* op 30 november 1999, die is georganiseerd door het ministerie van BZK, het Instituut voor Publiek en Politiek en het Electronic-highway Platform Nederland.

De eerste vraag die in dit kader beantwoord dient te worden is *waarom* zouden we eigenlijk elektronisch gaan stemmen. Daarna zal worden ingegaan op de technische vraag, *hoe* we elektronisch kunnen stemmen. Als laatste wordt ingegaan op de relatie tussen elektronisch stemmen en *privacy*.

Een eerste reden om elektronisch te stemmen is de verwachting dat elektronisch stemmen de opkomst bij verkiezingen zal vergroten. De legitimatie van de democratie en dus de legitimiteit van volksvertegenwoordigers hangt volgens politici, politicologen en bestuurskundigen onder meer samen met de opkomst bij verkiezingen. Wanneer de opkomstcijfers bij verkiezingen drastisch afnemen – zoals de lage opkomst bij de Provinciale Staten verkiezingen in 1999 – wordt hierover met de nodige bezorgdheid gesproken. Hoewel de advocaat van de duivel kan verdedigen dat een lage opkomst bij verkiezingen juist duidt op een ‘tevreden volk’, wordt een lage opkomst vaak geïnterpreteerd als een potentiële bedreiging voor de democratie. Daarom worden er van tijd tot tijd – meestal in het kader van bestuurlijke vernieuwing – voorstellen gedaan met het oog op het verhogen van de opkomst bij verkiezingen. Ook het kabinetsvoorstel van juli 1999 voor het op één dag houden van verschillende verkiezingen (bijvoorbeeld Gemeenteraad, Provinciale Staten en Tweede Kamer-verkiezingen) is hier een voorbeeld van.[34] In augustus 1999 is het Platform Elektronisch Stemmen (PELS) opgericht. Dit platform stelt voor burgers telefonisch of via internet te laten stemmen. Dit zal de legitimiteit van de democratie ten goede komen, aldus de oprichters van PELS. "Voornamelijk, omdat wordt verwacht dat de opkomst bij elektronische verkiezingen vanwege het gemak zal toenemen".

---

[34] De Raad voor het openbaar bestuur ondersteunt dit voorstel. Dit voorstel is besproken in een advies over de rol van de provincie, getiteld ‘Het bestuurlijk kraakbeen’, van december 1999.

Niet alleen de verwachte hogere opkomst, maar ook het gemak voor de burgers omdat elektronisch stemmen niet aan plaats gebonden is, vormt een argument voor elektronisch stemmen.
Als tweede reden voor elektronisch stemmen stelt het platform dat bij deze manier van stemmen *hippe* ICT-technieken worden toegepast en dat de overheid daardoor niet het risico loopt als ouderwets te worden beschouwd. De hoogleraar Bestuurskunde Tops onderstreept dit argument. In *Nieuwe media Burger en Bestuur* schrijft hij het volgende: "In deze context is elektronisch stemmen een grote vooruitgang, …, de daad van het stemmen is hiermee niet langer een ouderwetse en bedompte aangelegenheid, maar iets dat modern en bij de tijd is". De vergelijking tussen traditionele stemlokalen en elektronisch stemmen beschrijft hij als volgt: "Zoiets als rolschaatsen, dat vreselijk ouderwets is, en skaten, dat modern en sexy is".[35]

De volgende vraag is meer technisch georiënteerd en luidt "hoe kunnen we elektronisch stemmen". Wat zijn voorwaarden voor elektronisch stemmen en welke aanpassingen zijn nodig alvorens we elektronisch kunnen stemmen?
Het uitgangspunt is natuurlijk dat alle zorgvuldigheidseisen waaraan verkiezingen nu voldoen ook bij elektronisch stemmen worden gehandhaafd. Hierbij is het meest in het oog springend dat iedere stemgerechtigde burger net zoals bij traditionele verkiezingen maar één keer mag stemmen en dat zijn stem anoniem moet zijn. Aan deze vereisten kan naar verwachting met gebruik van technologie in de nabije toekomst worden voldaan. Prototypes van elektronische stemsystemen tonen aan dat het registeren en identificeren (m.b.v. biometrie) van een kiezer en tegelijkertijd anoniem stemmen mogelijk is. Hierbij geldt hetzelfde voorbehoud als in de sectie over centrale persoonsnummers. De overheidsidentificatiekaart op basis van biometrische gegevens is in ontwikkeling, wordt nog getest en wordt nog niet voor 100% vertrouwd. Maar anderzijds is ook het ‘oude systeem’ met de stemkaart ter identificatie niet waterdicht.
Registreren is van belang zodat elke kiesgerechtigde burger maximaal één keer kan stemmen. Identificatie is noodzakelijk zodat niemand de stem van een ander kan dupliceren of veranderen zodat geen fictieve stemgerechtigden zich aandienen. Een kiezer krijgt een kiessleutel (soort persoonlijke code). Hij of zij identificeert zich met een smartcard (waarop biometrische gegevens staan bijvoorbeeld een vingerafdruk) en de persoonlijke kiessleutel.
Vervolgens wordt de stem zodanig versleuteld dat niet meer te achterhalen is wie heeft gestemd en op wie is gestemd. Er is bij de prototypes ook voorzien in de mogelijkheid te controleren of de stem daadwerkelijk is uitgebracht.
Natuurlijk zijn er ook waarborgen ingebracht voor het beschikbaar zijn van de ‘verkiezingssite’ – de *site* mag niet *crashen* doordat er veel mensen tegelijk inloggen -, voor het zorgvuldig opslaan van de stemmen en voor het maken van *backup’s*.

---

[35] Tops, 1999.

Een volgend belangrijk aspect is het vormgeven van het virtuele stembureau. Dit lijkt eenvoudiger dan het is. Immers, als bovenstaande *high-tech* in de nabije toekomst mogelijk is, zou het ontwikkelen van een goede *interface* geen problemen mogen opleveren. Een punt van aandacht is echter dat bij gebruikmaking van *personal computers*, in tegenstelling tot de ouderwetse papieren kieslijsten of de lijst op de stemcomputers, niet alle partijen met daaronder alle verkiesbaren in één oogopslag te zien zijn. Een oplossing hiervoor is een computerscherm met eerst de verschillende lijsten en dan 'doorklikken', waarna de kandidaten van de betreffende lijst op het scherm verschijnen. Hierbij wordt het de burger moeilijk gemaakt – volstrekt legitiem – op een persoon te stemmen zonder te weten tot welke partij hij of zij behoort.
Met betrekking tot de *interface* dient vervolgens te worden opgemerkt dat de ontwerpen uitgaan van een *touchscreen*-systeem. Met het aanraken van de lijst of de kandidaat op het scherm kan de stem worden uitgebracht.[36] Hiervoor is geen typevaardigheid of 'muisvaardigheid' nodig.

Voor het technisch uitvoeren van het locatie onafhankelijk stemmen zijn nog veel aanpassingen nodig. Een veilige 'smartcard' met biometrische gegevens voor persoonlijke identificatie moet nog worden ontwikkeld. De apparatuur om thuis deze kaart op de computer te kunnen inlezen, moet bij burgers terecht komen. Natuurlijk zullen voor de niet-internetgebruikers of computerbezitters centra moeten worden ingericht waar kan worden gestemd. Een overgangstermijn met zowel stemlokalen als de mogelijkheid tot elektronisch stemmen is wenselijk. Een laatste noodzakelijke aanpassing is een wijziging van de Kieswet. Voordat met elektronisch stemmen kan worden begonnen moet de Kieswet worden veranderd.

Het goed verlopen van verkiezingen is een basisvoorwaarde voor een democratie. Zorgvuldigheid blijft ondanks enthousiasme en vernieuwingsdrift geboden. Als laatste beschouwen we de consequenties van het invoeren van elektronisch stemmen voor de privacy van de burger. We veronderstellen hierbij dat aan de technische vereisten voor identificatie en voor anoniem stemmen met te ontwikkelen technologie wordt voldaan. Een probleem met betrekking tot de privacy kan alleen nog ontstaan door de omgeving van het virtuele stembureau. Een garantie voor stemmen zonder beïnvloeding is er in de ontwerpen voor elektronisch stemmen niet. Hiervoor waarschuwt ook wetenschapper Van Dijk van de Universiteit Utrecht. Hij wordt in *Nieuwe media Burger en Bestuur* als volgt geciteerd: " Pa zegt dit en zoon stemt dit".[37]
In het traditionele systeem met toezicht in de kieslokalen kan iedere burger

---

[36] Dit is één van facetten in het systeem waarvoor aanpassing nodig is. Het werken met biometrie om je te identificeren en het gebruiken van touch-screen zijn technieken die ook bij de meeste mensen die thuis internetaansluitingen hebben, nog niet aanwezig zijn.

[37] Buurman, 1999.

geheim stemmen en heeft stemmen ronselen (weinig) geen kans, omdat toch niet gecontroleerd kan worden of iemand ‘doet wat hij zegt’. In het systeem waarbij vanuit het huis kan worden gestemd, zijn deze ontwikkelingen denkbaar. Ook de beïnvloeding van de kiezer bij het stemlokaal verandert. Verkiezingsposters hangen minimaal 10 meter bij het stemlokaal vandaan. In het virtuele stembureau zijn allerlei ‘links’ en beïnvloedingsmogelijkheden denkbaar.
Het is volgens de Raad onwenselijk dat in het stemlokaal – of dit nu fysiek of virtueel is – beïnvloeding mogelijk is. In een virtueel stembureau is het denkbaar dat er vanuit andere pagina’s op het net wordt ‘*gelinked*’. Dit zou er als volgt kunnen uitzien, "u vindt het leven van de zeehondjes op de Wadden belangrijk? Ja! Klik dan hier, en stem xxx". Een virtueel stembureau zou dus zodanig moeten worden ontwikkeld dat hieraan geen *hyper-links* kunnen worden verbonden.

De Raad is voorstander van elektronisch stemmen, mits aan de technische betrouwbaarheidseisen en aan een zorgvuldige inrichting van het virtuele stembureau wordt voldaan. Voorts is de Raad van mening dat voor de eerste paar verkiezingen een overgangstermijn met zowel mogelijkheden voor elektronisch stemmen als voor traditioneel stemmen op een stembureau van kracht dient te zijn.

Het ontwerpen van elektronische stemsystemen is een goede ontwikkeling, maar dient met de nodige behoedzaamheid te worden uitgevoerd. Immers, hierbij kan niet alleen de privacy van de burger in het geding komen, maar staat de legitimiteit van ons democratisch stelsel op het spel.

2.5
Samenvatting
De overheid, in haar rol als verzorgingsstaat waarbij het verlenen van diensten centraal staat, zal bij het uitoefenen van haar taken zich steeds bewust moeten zijn van haar omgang met gegevens en de relatie hiermee tot privacy. Informatievrijheid van burgers, vertaald in zeggenschap van burgers en een minimalistisch gegevensbeheer met goede autorisatieregels van de overheid, dient centraal te staan. De criteria genoemd door de burgers en vertaald in de WBP – zoals het voldoen aan doelbinding, transparantie, proportionaliteit, voorspelbaarheid en de informatieplicht – dienen te worden nageleefd. Op basis van de criteria uit de WBP en discussie met belanghebbenden dienen autorisaties te worden verleend. Een onderscheid is gemaakt tussen diensten met een verplicht karakter en diensten waarbij dit niet het geval is. Wanneer we bijvoorbeeld spreken over diensten in het kader van armoedebestrijding is de Raad van mening dat de burger zelf moet kiezen hiervoor al dan niet in aanmerking te willen komen. Om dit te bewerkstelligen zal de overheid de voorwaarden moeten scheppen om deze keuzemogelijkheid aan haar burgers kenbaar te maken.
Voor het praktische ontwerp van de informatiehuishouding zijn verschillende

alternatieven mogelijk. Een aanpak waarbij we uitgaan van decentrale gegevensbanken met verwijsindices kan zowel de efficiency als de effectiviteit van overheidsbeleid ten goede te komen en kan tegelijkertijd een goede waarborg vormen voor de privacy van de burger. Ditzelfde kan echter ook worden gezegd van landelijke gegevensbanken en bovensectoraal gebruik van persoonsnummers, mits zorgvuldig ingericht.

3.
‘ICT en privacy’ in de rechtsstaat

3.1
Inleiding

Het uitgangspunt van de overheid in de rechtsstaat is de waarborg van de individuele vrijheid van haar burgers. In de omgang met privacy van de overheid in de rechtsstaat komt een nieuw thema aan de orde. Niet alleen onderzoeken we de handelingsruimte van de overheid, maar beantwoorden we ook de vraag wie verantwoordelijk is voor het beschermen van de persoonlijke levenssfeer. Hierbij gaat de Raad uit van het denkbeeld dat de verantwoordelijkheid voor de bescherming van privacy een zaak van de burgers zelf is. Privacy is immers, zoals ook de vrijheid van meningsuiting, een klassiek en geen sociaal grondrecht en valt dus binnen de invloedsvrije sfeer van de overheid. Dit leidt tot de overtuiging dat de overheid een terughoudende rol moet spelen. Desalniettemin heeft de overheid in de rechtsstaat door haar taken als wet- en regelgever ook met betrekking tot de privacy een voorwaardescheppende rol.

Thema’s met betrekking tot ‘ICT en privacy’ in de private sfeer zijn *data-mining* en de groei van communicatie over internet. Wanneer we stellen dat de verantwoordelijkheid bij de burgers – lees consumenten – zelf ligt, moeten burgers ook zelf zorg dragen voor de bescherming van gegevens voor *data-mining* en bescherming van gegevensverkeer op internet. Hierbij kunnen burgers en overheid het aan de markt overlaten om te bepalen hoe gegeven de wet en de eisen van de klant praktisch dient te worden omgegaan met privacy in de informatiesamenleving.
Een voorbeeld van marktwerking in de informatiesamenleving is een bedrijf dat aan *e-commerce* doet en daarbij een *Trusted Third Party* (TTP) gebruikt voor het betalingsverkeer. Het betreffende bedrijf gebruikt de TTP niet uit nobele overwegingen, maar omdat consumenten veilige transacties eisen.

ICT-wetgeving samen met regels die door marktwerking zullen ontstaan, vormen de basis voor de omgang met privacy in de ICT-samenleving. De verhouding tussen ‘internet en privacy’ en ‘privacy in de commercie’ wordt in de eerste twee paragrafen van dit hoofdstuk bestudeerd.

De overheid als wetgever komt daarna aan de orde. Wetgeving over privacy – zoals we ook zagen in het tweede hoofdstuk, waar de WBP is geïntroduceerd – geeft een kader voor verwerking van persoonsgegevens. De wetgeving over privacy, zowel nationaal, internationaal als grondwettelijk, komt in deze sectie aan de orde. De verhouding tussen privacywetgeving en de privacywaarborgen in sectorale wetgeving – zoals bijvoorbeeld de Politiewet – komt ook aan de orde.
De taak van de overheid om de individuele vrijheid van de burger te beschermen, en haar bevoegdheid met betrekking tot opsporing en vervolging

van overtreders van wetten is een laatste aandachtspunt. Opsporing en vervolging van verdachten kunnen haaks staan op privacybelangen van burgers.

3.2
Internet

Een ICT-ontwikkeling in de private sector die invloed heeft op de privacy van burgers is de groei van informatie-uitwisseling, communicatie en handel (zowel marketing als verkoop van producten) via internet. Het aantal mensen met internet-aansluitingen is reeds ruim 130 miljoen. In Nederland heeft ongeveer 20% van de bevolking toegang tot internet. Ook de handel over het net is in de afgelopen jaren toegenomen. In 1999 bedroeg de omzet in elektronische handel in Nederland ongeveer 2,3 miljard. Naar verwachting zal de omzet in elektronische handel in Nederland de komende jaren sterk groeien en is dit een ontwikkeling waar rekening mee gehouden dient te worden.

Gezien het steeds groter wordende belang van internet in de samenleving is het niet verwonderlijk dat onveiligheid op internet breed in de belangstelling staat. De privacy van gebruikers van internet is onvoldoende gewaarborgd. Vandaag de dag vormt de *hacker* een mogelijke inbreuk op de privacy op internet.[38] Een *hacker* is iemand die in computers inbreekt en zich daarmee toegang tot computers verschaft. Een ‘echte’ *hacker* is gefascineerd door techniek en laat zich niet door hebzucht leiden, maar is gedreven om de feilbaarheid van de techniek bloot te leggen. Een andere ontwikkeling van deze tijd is dat iedere gebruiker, door te surfen op het net, *cookies* kan achterlaten. Een netwerkbeheerder plaatst dan een herkenningscode op de computer van de bezoeker van de *site*. Deze *cookies* zorgen ervoor dat de beheerder ‘de oude bekende’ herkent, wanneer deze weer langs surft. Hierdoor kunnen op persoonlijke voorkeuren afgestemde aanbiedingen worden gedaan. De gemiddelde surfer over het net is zich niet bewust van de sporen die hij of zij achterlaat. De *cookies* en het *tracken* van een gebruiker over het net – het surfgedrag nagaan – zijn bedreigingen voor de privacy van de gebruiker.

Om de privacy beter te beschermen is regulering nodig. De Raad is van mening dat de gebruiker en de aanbieder hiervoor primair zelf verantwoordelijk zijn. De privacy van de gebruiker van internet neemt toe wanneer een webbeheerder informatie geeft over zijn privacybeleid en wanneer de beheerder zijn *site* beschermt.[39] De consument heeft ook eigen verantwoordelijkheid en kan zelf zijn of haar communicatie op het net beveiligen. De Raad ondersteunt het streven naar anonimiteit en zelfredzaamheid van de gebruiker van internet. Dit sluit aan bij de norm dat een ieder ‘eigenaar’ is van zijn eigen gegevens. De

---

[38] stichting EPN, 1999.

[39] Een internetprovider stelt sinds kort een programma gratis ter beschikking aan zijn gebruikers. Dit programma maakt surfers anoniem. De provider biedt het programma aan omdat zij zegt te hechten aan de bescherming van de privacy.

Raad is tevens van mening dat de overheid kan bijdragen aan vergroting van de privacy door voorlichting te geven over (het gebrek aan) privacy op internet. Hierdoor kan de bewustwording van de consument worden vergroot.

Een ander soort probleem op internet betreft de (on)betrouwbaarheid van het betalingsverkeer. Identificatie van afzender en ontvanger is van groot belang om betrouwbaar zaken te kunnen doen. Hierbij kan een gebruiker dus vrijwillig afzien van anonimiteit, omwille van de 'veiligheid' van de transactie. Om de betrouwbaarheid te verhogen zijn allerlei oplossingen zoals biometrie, encryptie en TTP's mogelijk. Biometrie lijkt een goede oplossing, maar biedt op korte termijn geen soelaas, omdat nog geen standaard identificatiebewijzen met gebruikmaking van lichaamskenmerken in omloop zijn. TTP's en encryptie zijn wel al antwoorden op de roep om privacy. Creditcardbetalingen bij de meest populaire boekhandel op internet worden ook door middel van encryptie beveiligd.
Ook met behulp van encryptie is het betalingsverkeer over het net nog niet helemaal veilig. De versleutelingscode RSA van 512 bits – het wettelijke maximaal toegestane niveau van encryptie – waarmee onder andere betalingsverkeer op internet beveiligd wordt, is in augustus 1999, veel sneller dan verwacht, gekraakt. Ook de veelgebruikte *e-mail*-voorziening van Microsoft – *hotmail* – is onlangs gekraakt. Dit is van belang omdat via encryptie niet alleen betalingen maar ook *e-mail* kan worden beveiligd.

De overheid heeft er echter door haar handhavingsfunctie ook belang bij versleutelde berichten te kunnen ontsleutelen. *Trusted Third Parties* die als beveiliging voor een internetbedrijf werken zijn ook verplicht hun encryptiesleutel aan de overheid te verstrekken.

Kort samengevat is de Raad van mening dat veiligheid van communicatie en transacties via internet vooral voor rekening moet komen van gebruikers en aanbieders. Omdat het economisch belang van betrouwbaar verkeer over het net groot is, kan worden vertrouwd op het zelfregulerend vermogen van de markt.
De taak van de overheid is het scheppen van ruime wettelijke kaders. Zij dient zich te beraden over regels omtrent maximale versleuteling. Daarbij kan worden gedacht aan een systeem waarbij privacyovertredingen op internet strafbaar worden gesteld. Op deze laatste *issues* wordt in de volgende paragrafen teruggekomen.

3.3
Informatiewinning

Vervuilde bestanden, dat wil zeggen bestanden met persoonsgegevens die niet juist zijn, zijn een bron van zorg bij verwerking van gegevens. Problemen met elektronische databestanden kunnen ontstaan wanneer databestanden incompleet, onjuist, niet accuraat, of ontoegankelijk zijn. Bij dienstverlening kunnen vervuilde bestanden tot verkeerde beslissingen leiden, terwijl bij het analyseren

van gegevens met onjuiste bestanden foutieve conclusies kunnen worden getrokken. Ook het simpelweg verkeerd geregistreerd staan in een databestand kan een probleem vormen wanneer dit als privacyschending wordt ervaren. Voor het verwerken van persoonsgegevens is het dus van belang dat de informatieopslag zorgvuldig geschiedt.

Het verzamelen en opslaan van gegevens in een datawarehouse (of datapakhuis), in plaats van gegevens in operationele bestanden te laten staan, maakt gegevens toegankelijk voor nader onderzoek. Het toegankelijk maken van data is een moeilijke en tijdrovende taak. Het opslaan van gegevens in een datapakhuis zorgt ervoor dat gegevens die al in andere bestanden staan, zodanig worden gekoppeld dat deze voor onderzoek kunnen worden gebruikt.
De volgende karakteristieken beschrijven een datapakhuis[40]:

- gegevens worden los van de originele datasets opgeslagen;
- gegevens worden beschikbaar gemaakt voor de gebruiker;
- verschillende datasets worden geïntegreerd;
- gegevens worden in verschillende tijdsperioden onderverdeeld;
- gegevens worden per subject – bijvoorbeeld de klant – opgeslagen;
- gegevens worden zodanig opgeslagen en geordend dat een computergebruiker die geen expert is op het gebied van informatiesystemen, het datapakhuis kan gebruiken.

Datamining – informatiemijnbouw – wordt gebruikt om kennis te vergaren uit de datapakhuizen. In tegenstelling tot 'gewone mijnbouw' worden niet reeds bestaande 'kant en klare brokjes' informatie losgebikt, maar gaat een intelligent zoekprogramma aan de slag om verspreide 'brokjes' te zoeken en aan elkaar te plakken. Door samenvoeging en bewerking van gegevens ontstaat kennis.[41]
Lohman beschrijft *datamining* als volgt:
"Datamining, sometimes called knowledge discovery, …, can be defined as the non-trivial extraction of implicit, previously unknown, and potentially useful information from data. , …, In essence, datamining consists of performing several analyses on the available data to find unknown patterns, and this is done automatically"(p.48).[42]

Het ontdekken van patronen – zoals bijvoorbeeld klantenprofielen – is het doel van deze processen. Doordat *dataminingtechnieken* zodanig zijn ontworpen dat zonder sturing wordt gezocht naar mogelijke relaties tussen gegevens, in tegenstelling tot de meeste andere statistische technieken, is het aantal onderzochte relaties vaak heel groot. Dit kan leiden tot resultaten die niet bevredigend zijn, omdat relaties tussen veel verschillende factoren afhankelijk van

---

[40] Lohman, 1999.

[41] Borking, Artz & Van Almelo, 1998.

[42] Lohman, 1999.

elkaar – met veel mitsen en maren – worden gevonden. Een voorbeeld van een klantenprofiel, gevonden met behulp van *datamining* is: 'jongens tussen de 16 en 20 jaar oud, die een computer kopen, zullen in 70% van de gevallen, binnen twee weken een *joystick* kopen'.[43] Beleid afstemmen op dergelijke relaties is moeilijk, omdat het gaat om een kleine groep klanten en ook nog eens om een korte periode waarin beleid effectief kan zijn.

De vraag is of en wanneer informatie die door *datamining* is gegenereerd, kan worden toegepast. In zijn proefschrift betoogt Lohman dat informatie gegenereerd door *datamining* pas interessant is, wanneer deze onverwachte relaties blootlegt die tegelijkertijd tot beleid of acties kunnen leiden, en dat helaas aan deze twee vereisten niet vaak wordt voldaan. Als er onverwachte relaties worden gevonden, zijn deze vaak niet toepasbaar. Bovendien, als er onverwachte significante relaties worden gevonden, leidt dat vaak tot nieuw onderzoek naar het waarom van de samenhang of het veronderstelde causale verband. Ook in Lohman's *casestudy* – over de belastingdienst – bleken er weinig significante relaties te vinden te zijn en waren de gevonden relaties bovendien niet geschikt voor actie.

Datamining kan, indien succesvol, behalve klantenprofielen ook informatie opleveren over potentiële kopers, riskante verzekerden, potentiële fraudeurs bij de belastingdienst of potentiële rechthebbenden op bijvoorbeeld individuele huursubsidie. *Datamining* is echter niet de enige methode die kan worden en wordt gebruikt voor het creëren van profielen. Wanneer gebruikers van *datamining* of andere methodieken profielen gaan koppelen aan concrete personen, kan verwerking van gegevens problematisch zijn voor de privacy van de burger. Dergelijke analyses kunnen leiden tot bepaalde gedragingen. Deze gedragingen ofwel acties zijn misschien gebaseerd op de uitkomsten van *datamining* of andere technieken, wanneer dus beleid wordt gemaakt op basis van de gevonden relaties, maar deze gedragingen zijn geen logisch gevolg van *datamining*. Voorbeelden van gedragingen op basis van de uitkomsten van het creëren van profielen zijn: uitsluiting (geen abonnement of verzekering krijgen), risicoselectie (bij hypotheekverstrekking of verzekeringen) of *informatiestalking* (*direct-marketing* activiteiten).

De rechtsgronden voor *datamining* zijn veelal te vinden in het wetsartikel uit de WBP over 'verwerking ten behoeve van statistische of wetenschappelijke doeleinden'. Hieronder valt ook bijna al het markt- en opinieonderzoek waarbij gegevens worden verwerkt. Holvast betoogt dat de verwerking in deze gevallen bijna altijd verenigbaar is met eerdere doeleinden waarvoor de data zijn verzameld, omdat de profielen geen 'bepaalde personen' zijn.[44] In de praktijk is dit soms risicovoller dan bewerkingen waarbij de *output* persoonsgegevens

[43] Lohman, 1999.

[44] Holvast, 1999.

zijn. In het laatste geval gelden namelijk alle beperkende bepalingen van de privacywetgeving zoals doelbinding, geen onverenigbaarheid en het recht op verzet. Het feit dat een bepaald persoon in een profiel past kan, zelfs wanneer dit profiel is gecreëerd met anonieme gegevens, nadelige gevolgen hebben. Zo is het mogelijk dat iemand die in een postcodegebied woont met een laag gemiddeld inkomen, geen verzekering kan afsluiten of geen bezorging op krediet krijgt van een postorderbedrijf. Andere voorbeelden zijn profielen die worden vertaald naar individuen die in een categorie 'potentiële kopers' vallen en op basis daarvan post ontvangen (*informatiestalking*).

Artz, beleidsmedewerker van de Registratiekamer, bespreekt in het tijdschrift Informatie en Informatiebeleid, de invloed van de WBP voor *datamining* en *datawarehousing*.[45] In dit artikel worden kort de belangrijkste argumenten uit de achtergrondstudie over *datamining* van de Registratiekamer herhaald.[46] Van belang is dat de Registratiekamer vergeleken met Holvast de WBP 'strenger interpreteert'. De meest interessante toevoeging van Artz (1999) is de bespreking van het recht op menselijke tussenkomst bij geautomatiseerde beslissingen. Dit betreft artikel 42 van het wetsvoorstel WBP.[47] Hierover stelt hij het volgende: "Naast het reeds bekende recht op inzage en correctie kent de WBP het recht op verzet, het recht op menselijke tussenkomst bij geautomatiseerde beslissingen en het recht op mededeling van de logica. Op grond van het *recht op menselijke tussenkomst* heeft de betrokkene er recht op dat niet uitsluitend op grond van geautomatiseerde gegevensverwerking beslissingen worden genomen die hem of haar in aanmerkelijke mate treffen, zoals beslissingen over beroepsprestatie, kredietwaardigheid, betrouwbaarheid of gedrag".[48] Het maken van profielschetsen en het toerekenen van een profielschets is toegestaan. Het gemaakte profiel mag echter geen reden zijn voor negatieve besluitvorming over een persoon zonder menselijke tussenkomst. Door deze laatste toevoeging wordt het risico van het maken van profielen in het algemeen, en van *datamining* in het bijzonder, danig verkleind. Het wonen in een slecht betalend postcodegebied mag als zodanig worden gekenschetst, maar mag niet zonder menselijke tussenkomst leiden tot een negatieve beslissing omtrent het afsluiten van een verzekering.

Datamining en andere vormen van het maken van profielen kunnen leiden tot incorrecte of tot zeer complexe voorspellingen. Om deze reden wordt betoogd dat het effect van deze technieken niet dient te worden overschat. Enerzijds is dit waar en blijkt de toepasbaarheid van de profielen beperkter dan veelal gesuggereerd, anderzijds kunnen ook slechte voorspellingen een risico vormen. Als voorspellingen evengoed worden gedaan en incorrect zijn, of gebeuren op

---

[45] Artz, 1999.

[46] Borking, Artz & Van Almelo, 1998.

[47] WBP, EK 25 892, 1999-2000.

[48] Artz, 1999.

basis van rare kenmerken, kan dit tot onwenselijke situaties leiden.[49] Natuurlijk dient hierbij in acht te worden genomen dat ook hier geldt dat negatieve beslissingen niet zomaar zonder menselijke tussenkomst mogen worden genomen. Negatieve gedragingen zoals uitsluiting zijn volgens de WBP strafbaar, wanneer dit behoorlijke consequenties voor de belanghebbende betreft en alleen gebaseerd is op geautomatiseerde verwerking van gegevens. Bij oneigenlijke gedragingen op basis van onderzoek naar profielen of bij ander oneigenlijk gebruik van persoongegevens adviseert de Raad daarom sancties op te leggen. Als aan privacyschendingen een prijskaartje wordt gehangen, verruimt dit de mogelijkheden voor de publieke en private sector. Boetebevoegdheden door de overheid en mogelijke civiele schadeclaims kunnen privacyschending 'duur' maken. Hier wordt in de volgende paragraaf op teruggekomen.

Een van de acties als gevolg van het maken van profielen kan *informatiestalking* betreffen. Dit uit zich in *direct-marketing* activiteiten zoals reclamefolders op de deurmat, oplopende aantallen telefoontjes en overvolle *e-mailboxen*. De regels hiervoor zijn neergelegd in de WBP. Het ongevraagd ontvangen van een *mailing* of telefoongesprek wordt door sommige burgers gezien als een inbreuk op hun privacy. Als aanvulling op de regels uit de WBP (recht op verzet), adviseert de Raad daarom een jaarlijkse *mailing* te organiseren waarin de adressen van organisaties die NAWT bestanden doorverkopen – zoals de DMSA en de KPN[50] – staan en waarin de mogelijkheid wordt geboden om door middel van een antwoordkaartje aan te geven geen prijs te stellen op telefonische of schriftelijke colportage. Hierbij dient in acht te worden genomen dat een dergelijke voorziening natuurlijk veel geld kost, maar de Raad is van mening dat een toename van de privacybeleving hier tegenop weegt. In plaats van zelf een folder uit het rek bij het postkantoor te halen, wordt dan de consument eens per jaar in de gelegenheid gesteld aan te geven of hij of zij prijs stelt op deze vorm van verkoop.
Met betrekking tot *informatiestalking* door digitale colportage – de zogenaamde SPAM-mails – is op Europees niveau in een wetsvoorstel over *e-commerce* voorgesteld om een *opt-out* register aan te leggen. De Raad ondersteunt dit voorstel.

3.4
De overheid als wetgever

Een andere taak van de overheid is het maken van wetgeving en het toezien op

---

[49] Een voorbeeld van een 'mislukte actie' op basis van profielen is een gerichte actie van een supermarkt naar een klant die volgens zijn profiel hondenbrokken 'nodig zou moeten hebben', maar na de gerichte aanbieding van de hondenbrokken bleek bij de betreffende klant de hond overleden te zijn.

[50] DMSA en KPN zijn twee grote organisaties die Naam, Adres, Woonplaats en Telefoonnummer gegevens, de NAWT-bestanden, doorverkopen.

naleving daarvan. In deze paragraaf wordt kort ingegaan op de belangrijkste wetgeving inzake 'ICT en privacy'. Als eerste wordt gekeken naar de Grondwet. Daarna zal internationale wetgeving op het terrein van bescherming van persoonsgegevens worden bestudeerd. Als laatste worden de WBP en sectorale wetgeving beschouwd.

In februari 1999 is onder voorzitterschap van professor Franken de 'Commissie Grondrechten in het digitale tijdperk' opgericht.[51] Deze commissie heeft als taak de regering te adviseren met het oog op ontwikkelingen in de ICT bestaande grondrechten aan te passen en de wenselijkheid te onderzoeken van vaststelling van nieuwe grondrechten. Vooral de grondrechten waarbij informatie een rol speelt zijn van belang: de vrijheid van meningsuiting (artikel 7), het recht op privacy (artikel 10) en het communicatiegeheim (artikel 13).
Met betrekking tot artikel 7 geldt dat de meeste bescherming wordt geboden aan uitingen door de drukpers terwijl voor radio, televisie, openbare vertoningen en andere uitingsmiddelen zoals cd's en videotapes minder bescherming van de vrijheid van meningsuiting geldt. Wetgeving gericht op de vrijheid van meningsuiting over internet is wenselijk om te bepalen onder welk lid van artikel 7 communicatie via het net valt, en omdat communicatie via internet een grensoverschrijdend bereik heeft. Artikel 10 beschrijft het recht op bescherming van de persoonlijke levenssfeer en stelt regels voor het vastleggen en verstrekken van persoongegevens. De commissie onderzoekt of de bescherming van het verzamelen van persoonsgegevens uitgebreid zal moeten worden naar de bescherming van de gehele keten van verwerking van persoonsgegevens.
Artikel 13, dat het communicatiegeheim beschermt, betreft in de huidige Grondwet slechts het briefgeheim, telefoon- en telegraafgeheim. Dit betekent dat in de huidige wetgeving een *e-mail* over een telefoonlijn wel onder artikel 13 valt, terwijl een *e-mail* via de kabel valt onder de privacybescherming van artikel 10. Voor de nieuwe vormen van communicatie zoals de fax, de draadloze telefoons en het internet, is aanpassing van de wet nodig.
De aanpassing van grondrechten is dus gericht op artikel 7, 10 en 13. De commissie mag ook, indien zij dit nodig acht, voorstellen doen voor het ontwikkelen van nieuwe grondrechten. Bij het instellen van nieuwe grondrechten wordt gedacht aan een grondrecht inzake toegang tot elektronische (overheids)informatie.[52]

Bij het ontwikkelen van nieuwe grondrechten en het aanpassen van de bestaande rechten streeft de commissie ernaar deze rechten zoveel mogelijk techniek-onafhankelijk te formuleren. Zeker gezien de snelle ontwikkelingen in de ICT vindt de Raad dit een zinvol streven. Vervolgens is de commissie van

---

[51] 'Commissie Grondrechten in het digitale tijdperk', 1999, www.minbzk.nl/gdt/.

[52] Wetgeving voor de elektronische snelweg. TK 25 880, 1998-1999.

mening dat het onderscheid tussen besloten communicatie (bijvoorbeeld een telefoongesprek) en openbare communicatie (bijvoorbeeld de omroep) het beste kan worden gehandhaafd. Verschillende grondrechten voor openbare en gesloten informatie lijkt de Raad, gezien de verschillende privacybehoefte van beide, zinvol. Dit onderscheid kan waarschijnlijk worden gemaakt zonder dat de wetgeving daardoor techniek-afhankelijk wordt. Er wordt in de commissie ook gesproken over het vervangen van het recht op privacy met het recht op anonimiteit. Dit laatste kan bijvoorbeeld betekenen dat iemand anoniem op internet mag surfen. Ondanks dat anonimiteit op internet ook nadelige consequenties kan hebben, gedacht kan worden aan gevaren van kinderporno op het net, is de Raad een voorstander van anonimiteit op internet. De andere kant van deze medaille is immers dat wetsovertreders ook zonder een aanpassing van de Grondwet zich dit recht op anonimiteit al (proberen te) toe-eigenen.
De commissie zal tevens letten op overeenstemming met bestaande wetgeving en wetsvoorstellen op het terrein van ICT. In een wetsvoorstel (strafrecht) van juli 1999 over computercriminaliteit wordt bijvoorbeeld voorgesteld *e-mail* onafhankelijk van het gebruikte transportmiddel te beschermen. Dit voorstel is elektronische post op dezelfde wijze te beschermen als de brief (zie artikel 13 Grondwet).
Er dient echter te worden opgemerkt dat alle besproken ideeën van de commissie nog in een ontwerpfase zijn. De commissie zal medio 2000 haar advies uitbrengen.

In internationaal verband zijn de aanbevelingen van de OESO "inzake bescherming van de privacy en de internationale uitwisseling van persoonsgegevens" en de Europese richtlijn "betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van gegevens", van belang. Hierbij dient te worden opgemerkt dat de OESO-richtlijn (1980) geen bindende werking heeft. Het doel van de richtlijn wordt als volgt beschreven: *the OECD members clearly intend to "help to harmonise national privacy legislation and, while upholding such human rights, to prevent at the same time interruptions in international flows of data*".[53] Een nieuwe OESO-richtlijn (1997) betreft een internationale richtlijn voor cryptografiebeleid, waarbij nationale overheden voor het ontwikkelen van beleid op het terrein van versleutelen van gegevens deze richtlijn als hulpmiddel kunnen gebruiken. Een dilemma bij cryptografie is dat aan de ene kant overheden versleuteling stimuleren om gegevens te beschermen, maar anderzijds willen voorkomen dat misdadigers cryptografie gebruiken om uit handen van de overheid te blijven. Het dilemma betreft dus privacy enerzijds en opsporing anderzijds. Deze vraagstelling is eerder gesignaleerd en hier wordt in de volgende paragraaf op teruggekomen. De Raad acht het betreurenswaardig dat ook de OESO- richtlijn niet aangeeft waar de balans moet liggen

[53] OECD privacy richtlijn, www.oecd.org.

tussen privacybescherming en overheidstoegang.
De Europese privacyrichtlijn – in Nederland vertaald in de WBP – voorziet in speelruimte voor het nationale recht en geeft ook individuele lidstaten de vrijheid sectorale wetgeving te ontwikkelen. In Nederland is met betrekking tot de privacy niet alleen de WBP ontwikkeld, maar zijn ook de Wet geneeskundige behandelings-overeenkomst, de Politiewet, de Algemene bijstandswet en de Wet GBA van kracht.
In de WBP zijn de regels voor publieke en private sector aan elkaar gelijkgesteld. Slechts materiële wetten – bijvoorbeeld de Algemene bijstandswet – kunnen de overheid bevoegdheden verlenen die voor de private partners niet gelden.

De belangrijkste voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens uit het wetsvoorstel WBP – zie artikel 6 tot en met 24 – zijn bestudeerd in hoofdstuk twee van dit advies. In deze paragraaf zal daarom niet op de voorwaarden voor verwerking worden ingegaan, maar zal de aandacht worden gericht op de naleving van de WBP. Het College bescherming persoonsgegevens kan (nu nog de Registratiekamer) als adviseur, controleur en in geval van conflicten als bemiddelaar dienen. Organisaties die gegevens verwerken, dienen dit aan te melden bij het College dat vervolgens toetst of de verwerking binnen de regels van de wet valt. Verder is het College ook nauw betrokken bij het ontwikkelen van normen en kan zij gedragscodes goedkeuren. In geval van geschillen tussen private partners zal het College bemiddelen. Tot nu toe blijkt een uitspraak van de Registratiekamer voldoende voor het oplossen van het geschil.

In het wetsvoorstel WBP is naast de reeds van kracht zijnde bestuursdwang ook een bestuurlijke boete van ten hoogste tienduizend gulden, op te leggen door het College, opgenomen. De handhaving van de WBP zal dus plaatsvinden op basis van bestuurlijke dwang, indien nodig bestuurlijke boeten, en als ultimum remedium op basis van strafrechterlijk optreden. Het College kan zelf of namens de *betrokkene* bestuursrechtelijk aanspreken. Als het College van mening is dat een *verantwoordelijke* (in WBP-zin) zich niet heeft gehouden aan bijvoorbeeld de meldingsplicht voor het verwerken van persoonsgegevens, kan het College hier een onderzoek naar instellen. In geval van onrechtmatige verwerking kan het College volgens het wetsvoorstel een bestuurlijke boete opleggen. Deze boetebevoegdheid vervalt indien tegen de overtreding door het OM al strafvervolging is ingesteld. Andersom, indien het College al een boete heeft opgelegd kan hetzelfde feit niet strafrechtelijk worden vervolgd.

De mogelijkheid een boete op te leggen door de overheid wordt door de Raad positief beoordeeld. De Raad vraagt zich echter af of deze bevoegdheid in handen van een toezichthoudend orgaan dient te komen. De mogelijkheid om, indien nodig via het strafrecht op te treden, wordt door de Raad positief beoordeeld.

Bij bovenstaande voorbeelden kunnen privacyschendingen ofwel onrechtmatig gebruik van persoonsgegevens wel worden bestraft, maar de *betrokkene* wordt er niets wijzer van. De Raad pleit daarom ook voor privaatrechtelijk optreden in geval van privacyschending. Indien het privacybelang van een betrokkene aanzienlijk wordt geschaad, en de betrokkene hiervan materiële (bijvoorbeeld een hogere verzekeringspremie op grond van risicoselectie) of immateriële schade oploopt zou de betrokkene de verantwoordelijke moeten kunnen aanspreken. Wanneer er op grond van de privacyschending sprake is van een onrechtmatige daad kan de betrokkene een schadeclaim indienen bij de verantwoordelijke. Deze gang van zaken zal de privacy in het algemeen ten goede komen. Dit privaatrechterlijk optreden past ook in het stramien van dit advies waarbij zelfregulering een belangrijke rol speelt. Bij dit soort optreden kan een burger zowel zijn eigen belang – zijn informatievrijheid – verdedigen, als benadrukken dat privacy geen gratis 'goed' is.

De Raad is van mening dat het van groot belang is dat privacyschending niet kosteloos is. Hij beoordeelt daarom bestuursdwang, strafrechtelijke sancties en de mogelijkheid voor schadevergoedingen positief.

In de kabinetsnota *Wetgeving voor de elektronische snelweg*, die is ontwikkeld met het doel beleidslijnen uiteen te zetten voor het legitimeren van de rol van de overheid in de informatiesamenleving, is ook gesproken over handhaving van het recht.[54] De belangrijkste conclusies in de kabinetsnota komen sterk overeen met hetgeen in dit advies is voorgesteld. Deelname in het elektronisch verkeer treft in eerste instantie de verantwoordelijkheid van aanbieders en gebruikers zelf. Verder is voor de overheid een faciliterende rol weggelegd. Voorstellen voor juridische normen betreffen in het algemeen het motto 'wat *off-line* geldt moet ook *on-line* gelden', en er worden voorstellen gedaan om ontwikkelingen als biometrie,[55] *Trusted Third Parties* (TTP) en *Privacy Enhancing Technologies* (PET) te faciliteren.
Ook het kabinet is dus van mening dat in de informatiesamenleving zelfregulering voorop staat en dat voor de overheid een ondersteunende – soms faciliterende – rol is weggelegd.

3.5
De overheid als handhaver; opsporing en vervolging

Een van de kerntaken van de overheid is zorg te dragen voor een veilige samenleving. Een discrepantie bestaat tussen het bestrijden van de misdaad en het waarborgen van een veilige maatschappij enerzijds en de inbreuk op de privacy van de burger door eerstgenoemde doelstelling anderzijds. Deze tweestrijd tussen 'ICT en privacy' in het kader van opsporing en vervolging

---

[54] Wetgeving voor de elektronische snelweg. TK 25 880, 1998-1999.

[55] Biometrie is het vaststellen van een meetbaar fysiek kenmerk of persoonlijk kenmerk om met geautomatiseerde middelen de identiteit vast te stellen

wordt in deze paragraaf bestudeerd. Ook zal in deze paragraaf nogmaals worden ingegaan op cryptografie.

De informatiseringmaatschappij zorgt voor nieuwe vormen van criminaliteit en voor nieuwe opsporingsmogelijkheden. Voor handhaving van het recht op de elektronische snelweg zijn de volgende uitgangspunten beschreven in de Nota wetgeving op de elektronische snelweg:
- gedragingen die *off-line* strafbaar zijn, zijn *on-line* evenzeer strafbaar;
- er dient een zorgvuldige afweging te worden gemaakt tussen het belang van de rechtshandhaving en de inbreuk die wordt gemaakt op de privacy van de burger;
- de ontwikkeling van de elektronische snelweg wordt zoveel mogelijk overgelaten aan de markt.

De Raad deelt in grote lijnen de uitgangspunten uit de kabinetsnota. In dit advies is reeds gepleit voor een toename van zelfregulering. Bovendien lijkt het de Raad vanzelfsprekend dat gedragingen die strafbaar zijn in het fysieke leven, dat ook zijn op internet. Over de afweging tussen rechtshandhaving en privacy is de Raad net als het kabinet van mening dat deze zorgvuldig dient te worden gemaakt, alleen geeft de Raad hieraan een andere invulling.

De afweging tussen rechtshandhaving en privacybescherming komt nadrukkelijk aan de orde wanneer we het cryptografiebeleid van de overheid bestuderen. De overheid heeft een maximaal niveau van versleuteling vastgesteld in het kader van de veiligheid. Omdat hogere belangen van de overheid voorrang krijgen, mag niet met meer dan 512 bits worden versleuteld. Bovendien moeten de zogenaamde TTP's, die cryptografie toepassen, hun sleutels inleveren bij de overheid. Versleuteling is toegestaan met als restrictie dat indien hogere belangen (o.a. staatsveiligheid, voorkoming, opsporing en vervolging van strafbare feiten) dat vergen, de gegevens terug te herleiden zijn naar concrete personen. Daarom is een bovengrens ingesteld.
Deze conflicterende belangen tussen veilig digitaal verkeer, privacybescherming en veiligheid zijn niet alleen in Nederland terug te vinden. Ook in de internationale richtlijnen van de EU en de OESO wordt dit probleem onderkend, echter het probleem wordt niet opgelost. In 'IT & Recht' verwijst Koops naar de OESO-richtlijn als een 'richtlijn zonder richting'.[56] Elke staat moet nog steeds zelf de balans vinden (zoeken) tussen beschermingsprincipes (privacy) aan de ene kant, en overheidstoegang (i.v.m. veiligheid) aan de andere kant. In Nederland is er dus sprake van een bovengrens op cryptografie tezamen met overheidstoegang tot cryptografische sleutels. In de nota wetgeving op de elektronische snelweg wordt gepleit voor verschillende normen voor cryptografie voor commercieel gebruik en voor overheidsdiensten als legers en ambassades. Hierover zegt de Registratiekamer het volgende: "De

[56] Koops, 1997.

beschikbaarheid van encryptie is van essentieel belang voor het vertrouwen van burgers en maatschappelijke organisaties in de digitale snelweg. Het belang van de opsporings- en veiligheidsdiensten om gecodeerde berichten te kunnen ontcijferen, weegt daar niet tegen op".[57]

De Raad begrijpt de wens van de overheid een maximaal niveau van versleuteling in te stellen. Echter, de Raad vreest dat het doel van het instellen van deze bovengrens – namelijk het kunnen ontcijferen van berichten voor opsporing en vervolging – niet wordt bereikt. Degenen die zich bezighouden met strafbare activiteiten zullen zich door deze regels niet laten weerhouden om meer dan de toegestane cryptografie toe te passen, en zullen hun 'sleutels' niet inleveren. Terwijl het toestaan van cryptografie, zonder dit aan banden te leggen, voor de veiligheid op de digitale snelweg juist goede effecten heeft. Het voorstel van de Raad cryptografie niet aan banden te leggen komt dus niet alleen voort uit een 'negatief argument', namelijk 'het helpt toch niet', maar ook uit een positieve, namelijk het versterken van de veiligheid en daarmee de privacy in het digitaal verkeer. Communicatie en transacties over het net kunnen met behulp van toepassing van cryptografie veilig worden.

Vanuit praktisch oogpunt gezien is er nog een argument voor het toestaan van ongelimiteerde cryptografie, namelijk het gegeven dat controle houden op het verkeer over internet enorm complex is. Hierbij kan worden gedacht aan de rol van de internetprovider. Is de provider verantwoordelijk voor het verkeer dat via hem loopt? Vooralsnog biedt wetgeving hierover weinig duidelijkheid. Onderscheid wordt gemaakt tussen *host- en serviceproviders* en er wordt vooral ingezet op zelfregulering.[58] De Raad vergelijkt de positie van een internetprovider met de telefoonaanbieder op het vaste net (de KPN) en is daarom van mening dat de provider niet verantwoordelijk kan worden gehouden. De telefoonaanbieder is immers ook niet verantwoordelijk voor de

---

[57] Registratiekamer, april 1998.

[58] Verschillende nationale en internationale ontwikkelingen met betrekking tot het ontwerpen van wetgeving over *e-commerce* lopen door elkaar heen. Er is een voorstel voor een richtlijn (EU) van december 1999 die juridische aspecten van *elektronic commerce* regelt en er wordt gewerkt aan het omzetten van twee verdragen (ook EU) op het gebied van internationaal privaatrecht. In de richtlijn (voorstel) geldt het '*country of origin*' principe, wat betekent dat de aanbieder zich moet houden aan het recht van het land waar hij is gevestigd. Met betrekking tot verantwoordelijkheid van providers voor het gedrag van hun klanten is het volgende voorgesteld: traditionele *serviceproviders* die toegang op het net aanbieden zijn niet verantwoordelijk voor wat hun klanten *on-line* doen, terwijl *hostproviders* wel verantwoordelijk worden geacht voor de inhoud van *sites* die klanten bij hun stallen. Deze *hostprovider* is verplicht – zodra hij ontdekt dat een klant illegale zaken aanbiedt – die *site* te verwijderen. Op nationaal niveau wordt bij de wet op de computercriminaliteit (II) gesteld dat handhaving inderdaad problematisch is en wordt zelfregulering van *service-providers* gestimuleerd.

berichten die over telefoonlijnen worden uitgewisseld. Zelfregulering van internetproviders kan wel een rol spelen; de providers kunnen 'illegale boodschappen' op (hun deel van) internet verwijderen.
De overheid kan, in haar opsporingsfunctie, telefoonlijnen afluisteren. Dit soort strategieën is op internet veel lastiger; simpelweg door de veelheid van aanbieders van 'digitale kanalen' is het moeilijk communicatie op internet te volgen wanneer iemand niet 'achtervolgd' wil worden. Een laatste reden om cryptografie niet aan banden te leggen is dus een praktische. Als iets niet te reguleren valt, is het ook verstandiger dit niet te proberen.

Om bovenstaande praktische reden, omwille van privacy, en voor veiligheid van communicatie en transacties op internet, geeft de Raad de voorkeur aan ongelimiteerde cryptografie boven het stellen van een bovengrens en het verplicht verstrekken van de sleutels.

De opkomst van ICT brengt zijn eigen criminaliteitsbeeld met zich zoals de aantasting van het goed functioneren van informatiesystemen (bijvoorbeeld door het binnendringen van computers of netwerken), vermogensdelicten (zoals creditcard fraude of het illegaal binnenhalen van en niet betalen voor betaaltelevisie) en uitingsdelicten (kinderpornografie of racistische literatuur).[59]

ICT-ontwikkelingen zorgen ook voor nieuwe opsporingsmethoden. Specifieke wetgeving in het kader van opsporingsbevoegdheden zoals bijvoorbeeld het aanleggen van een telefoontap of het verstrekken van persoonsgegevens, zijn een gevolg van informatisering en tegelijkertijd een belemmering voor de persoonlijke levenssfeer van burgers. De strafrechtelijke wetgeving gaat in het algemeen, omwille van de openbare orde, verder in het aantasten van de persoonlijke levenssfeer dan is toegestaan volgens de bepalingen in de WBP. Minister Korthals van Justitie heeft in juli 1999 aan de Tweede Kamer laten weten dat er nieuwe eenduidiger regels moeten komen voor het verstrekken van informatie aan de politie. Hierbij gaat het om het verstrekken van persoonsgegevens door zowel internetproviders, telecomaanbieders, banken, vervoersbedrijven en winkeliers. In het voorstel van Korthals zullen deze bedrijven zonder tussenkomst van een rechter-commissaris vertrouwelijke gegevens moeten verstrekken. De Raad vindt dat de vraag of gegevens al dan niet moeten worden verstrekt aan de politie, onafhankelijk van de vraag of dit een fysieke of digitale bron betreft, dient te worden beantwoord. Het verstrekken van informatie uit het schriftelijke klantenbestand van een winkelier is volgens de Raad hetzelfde als het verstrekken van informatie door een telecom- of internetaanbieder.

---

[59] Een uitgebreide beschrijving van internetdelicten is te vinden in een tweetal publicaties van de Stichting Maatschappij, Veiligheid en Politie: 'Fraude en het Internet' en het achtergrondrapport 'Achtergronden van Internetfraude', maart 1999.

De overheid is zowel wetgever, handhaver als potentiële overtreder van de wet op de privacy. Er zijn, zoals gezegd, als gevolg van de digitale revolutie nieuwe opsporingstechnieken zoals het surveilleren op internet, het afluisteren van mobiele telefoons, het (drie maanden) bewaren van alle GSM gesprekken, en de ontwikkeling van DNA (misdaad)databanken. De handhaving van de openbare veiligheid lijkt, bijvoorbeeld gezien de regels met betrekking tot cryptografie, door de overheid prioriteit te krijgen. De overheid wil enerzijds de privacy van haar burgers beschermen, maar wil tegelijkertijd het liefst alle digitale verkeer kunnen volgen. Hierdoor lijkt de overheid soms een hoger belang toe te kennen aan openbare orde dan aan privacy. Hierbij dient echter te worden opgemerkt dat dit niet alleen de overheid betreft, maar ook burgers geven het maatschappelijk belang van veiligheid soms voorrang boven privacy.

De Raad stelt daarom dat ook bij opsporing en vervolging rekening gehouden dient te worden met privacy en dat regels voor opsporing en vervolging in het digitale tijdperk gelijksoortig dienen te zijn als in het 'fysieke tijdperk'. Het kabinet dient zich terdege bewust te zijn van alle nieuwe ontwikkelingen en als gevolg daarvan nieuwe delicten en nieuwe opsporingsmogelijkheden, maar dient haar wetgeving zoveel mogelijk onafhankelijk van de techniek op te stellen. Zo dient bijvoorbeeld de vraag of *tracking* van personen door middel van het volgen van een mobiele telefoon is toegestaan niet van het middel – het achtervolgen via signalen die worden opgevangen door satellieten -, maar van de rechtmatigheid van de achtervolging af te hangen.

3.6
Samenvatting

Het eerste thema dat in dit hoofdstuk is besproken is privacy op internet. Hierbij is gepleit voor zelfregulering van gebruikers en aanbieders. Met betrekking tot datamining en andere vormen van het maken van profielen blijkt dat dit in het nieuwe wetsvoorstel – de WBP – goed is geregeld, hoewel gewaarschuwd wordt voor ruime interpretatiemogelijkheden van de WBP op dit terrein. De wetgeving inzake 'ICT en privacy' is aan vernieuwing toe. Een commissie is aangesteld om de regering over aanpassing van de grondrechten te adviseren, en Europese wetgeving over privacy wordt vertaald in de nieuwe WBP. Techniek-onafhankelijke wetgeving en het invoeren van een boete voor privacyschendingen, worden door de Raad ondersteund. Bij de handhaving van openbare orde en veiligheid dient de regering rekening te houden met nieuwe mogelijkheden voor delicten en voor opsporing. Voor beide geldt dat wat strafbaar of toelaatbaar is onafhankelijk dient te zijn van de technische toepassing. Verder is de Raad van mening dat een bovengrens op cryptografie niet het juiste antwoord op de afweging privacy versus veiligheid is.

4.
Conclusies en Aanbevelingen

4.1
Conclusies

Over de vraag hoe de overheid moet omgaan met ICT-ontwikkelingen in relatie tot privacy en over verantwoordelijkheid voor bescherming van privacy is in deze nota geadviseerd.

Met betrekking tot de rol van de overheid in de verzorgingsstaat is geconcludeerd dat de overheid op een verantwoorde wijze moet omgaan met gegevensverwerking. Hierbij is primair informatievrijheid en -eigendom van de burgers het uitgangspunt. Een onderscheid is gemaakt tussen verplichte – en vrije diensten. Alleen bij de laatste vorm van dienstverlening kan en dient informatie-eigendom ten volle te worden gehonoreerd. De overheid dient steeds uit te gaan van een zo minimaal mogelijke gegevensverwerking. Actief zal hiervoor moeten worden gewerkt aan bewustwording bij de overheid zelf. Aan de criteria voor een verantwoorde omgang met gegevens, zoals genoemd door de burgers en beschreven in de WBP, namelijk proportionaliteit, doelbinding, transparantie en voorspelbaarheid, moet worden voldaan. Een opmerkelijk gegeven is dat burgers privacy in zijn algemeenheid niet als probleem beschouwen, maar wel hun privacy in specifieke relaties. Daarom is de Raad van mening dat met beantwoording aan de vereisten in de WBP voldoende bescherming van de persoonlijke levenssfeer kan worden bereikt. Om een goede balans tussen het gebruik van persoonsgegevens en privacy te vinden, zijn zowel een cultuurverandering bij de overheid als bedrijfsleven, als het inzetten van instrumenten zoals ‘minimalistisch gegevensbeheer’, ‘ontkoppeld koppelen’, ‘het verstrekken van gegevensoverzichten’ en ‘voorlichting’ nodig. Door het invoeren van deze instrumenten schept de overheid de voorwaarden waardoor een burger zijn ‘eigen verantwoordelijkheid’ voor de bescherming van zijn privacy ook kan nemen.
Voor het praktische ontwerp van de informatiehuishouding zijn verschillende alternatieven mogelijk. Voorlopig lijkt een aanpak waarbij wordt uitgegaan van decentrale gegevensbanken en verwijsindices, zowel de efficiency als de effectiviteit van overheidsbeleid ten goede te komen en tegelijkertijd een goede waarborg te vormen voor de privacy van de burger.
Het uitgangspunt bij het locatie-onafhankelijk elektronisch stemmen is natuurlijk dat alle zorgvuldigheidseisen waaraan verkiezingen nu voldoen, ook bij elektronisch stemmen worden gehandhaafd. Hierbij is het meest in het oog springend dat iedere stemgerechtigde burger net zoals bij traditionele verkiezingen, maar één keer mag stemmen en dat zijn stem anoniem moet zijn. Aan deze vereisten kan met gebruik van technologie worden voldaan. De Raad is voorstander van het invoeren van elektronisch stemmen. Er is door de Raad echter ook gewezen op mogelijke nadelige consequenties door de inrichting van een elektronisch stemlokaal zoals beïnvloeding en ronselen van stemmen. Hierbij kan niet alleen de privacy van de burger in het geding komen, maar

staat ook de legitimiteit van ons democratisch stelsel onder druk.

Het uitgangspunt van de overheid in de rechtsstaat, besproken in het derde hoofdstuk, is de waarborg van individuele vrijheid van haar burgers. Hierbij is niet alleen de handelingsruimte van de overheid bestudeerd, maar ook de vraag wie verantwoordelijk is voor het beschermen van de persoonlijke levenssfeer beantwoord. Hierbij stelt de Raad voorop dat de verantwoordelijkheid voor de bescherming van privacy primair een zaak van de burgers zelf is. Hiervoor dient de overheid wel, net zoals in de verzorgingsstaat, randvoorwaarden voor de burgers te scheppen zoals het strafbaar stellen van privacyschending, het verruimen van kansen en rechten op anonimiteit en veilige transacties op internet, en meer in het algemeen door het actualiseren van wetgeving.
Het eerste thema dat is besproken is privacy op internet. Hierbij is gepleit voor zelfregulering van gebruikers en aanbieders.
Met betrekking tot het creëren van profielen onder meer door *datamining*, blijkt dat dit in het nieuwe wetsvoorstel – de WBP – redelijk goed is geregeld. Er is echter ruimte voor interpretatie in de WBP, maar het artikel in de WBP over 'het recht van menselijke tussenkomst bij geautomatiseerde beslissingen', zal nadelige consequenties van *datamining* beperken.
In het algemeen is met betrekking tot de wetgeving inzake 'ICT en privacy' geconstateerd dat deze aan vernieuwing toe is. Een commissie is reeds aangesteld om de regering over aanpassing van de grondrechten te adviseren en de Europese richtlijn over privacy wordt vertaald in de nieuwe WBP. In dit kader worden ook voorstellen voor techniek-onafhankelijke wetgeving en het invoeren van strafrechtelijke sancties en mogelijkheden voor schadevergoedingen voor privacyschendingen, door de Raad ondersteund.
Bij de handhaving van openbare orde en veiligheid dient de regering rekening te houden met nieuwe (ICT-)mogelijkheden voor delicten en voor opsporing. Voor beide geldt dat wat strafbaar of toelaatbaar wordt geacht, onafhankelijk dient te zijn van de technische toepassing. Voorts is de Raad van mening dat een bovengrens op cryptografie niet het juiste antwoord op de afweging 'privacy versus veiligheid' is.

Het antwoord op de vraag 'hoe de overheid moet omgaan met de afweging tussen het gebruik van ICT en privacy' in de informatiseringssamenleving valt samen met de vraag wie verantwoordelijk is voor de bescherming van de privacy. Voorop staat de informatievrijheid en dus de zeggenschap van de burgers. Gepaste afstand van de overheid tot de burger en gedeelde verantwoordelijkheid is daarom geboden. Het uitwerken van de criteria genoemd in de WBP en toepassen van de instrumenten die in dit advies zijn genoemd – zowel instrumenten waarbij de overheid de privacy van de burgers beschermt als wel instrumenten die zelfregulering van burgers bevorderen – zullen bijdragen aan een goede omgangsvorm voor de overheid in relatie tot 'ICT en privacy'.

4.2
De kernvragen beantwoord

In dit advies is een kader geschapen om de vragen uit de adviesaanvraag te beantwoorden. Ter herinnering herhalen we de vragen uit de adviesaanvraag.

- Welke verschillende opties bestaan er voor de overheid om binnen het kader van de toekomstige WBP in het algemeen om te gaan met het privacybegrip (bijvoorbeeld persoonsnummers) en wat betekent dit voor het handelingsvermogen van de overheid?
- Betekent meer handelingsvermogen vanzelf minder privacy of zijn er ook mogelijkheden om door een andere wijze van omgaan met persoonsgegevens meer handelingsvermogen te realiseren met evenveel of zelfs meer privacy?
- Welke posities hebben basisregistraties in de overheidsinformatiehuishouding ten opzichte van sectorale indexen die zich ontwikkelen tot centrale registers met algemene gegevens?

De eerste vraag betreft *de opties van de overheid voor het omgaan met privacy binnen de kaders van de WBP*. Deze vraag suggereert een grote mate van beleidsvrijheid binnen de nieuwe wetgeving. Om de mogelijke opties – en dus de beleidsruimte – te bestuderen, bespreken we twee uitersten.

Als de overheid binnen de WBP haar handelingsruimte, eventueel ten koste van de privacy, zoveel mogelijk wil uitbreiden, zijn daarvoor de volgende mogelijkheden aanwezig. Ten eerste zal de overheid de bepalingen in de WBP zo ruim mogelijk uitleggen. Juist de artikelen waarbij een zekere mate van ambiguïteit aanwezig is, zoals de bepaling dat gegevensverwerking ‘niet onverenigbaar’ met het oorspronkelijke doel van gegevensverwerking mag zijn (art. 9) of de bepaling over informatieverstrekking aan de betrokkene waarbij de betrokkene niet op de hoogte wordt gesteld van de verwerking indien dit ‘onmogelijk blijkt of onevenredige inspanning kost’ (art. 34), zijn voor ruime interpretatie vatbaar. In het kader van zoveel mogelijk handelingsruimte is een tweede middel van de overheid zich niet meer in te spannen voor de bescherming van de privacy dan absoluut noodzakelijk (ofwel wettelijk verplicht) is. De overheid kan tevens via het invoeren van sectorale wetgeving die de kaders van de WBP overschrijdt, zoals bijvoorbeeld de Politiewet, haar handelingsruimte vergroten. In het kader van de Politiewet zijn privacyschendingen mogelijk die op grond van de WBP niet aanvaardbaar zijn.

Het andere uiterste is op grond van de WBP alle mogelijke initiatieven te blokkeren op grond van mogelijke privacyschendingen. Hierbij kan worden gedacht aan het niet invoeren van pro-actieve dienstverlening en elektronisch stemmen onder het motto van privacybescherming.

Beide extreme opties zijn onwaarschijnlijk. In een samenleving waar consensus regel is, wordt naar een middenweg gezocht. Hierbij wordt gerefereerd aan de voorstellen die in dit advies zijn gedaan. De WBP moet

allereerst nauwlettend worden gevolgd en hierbovenop is een aantal aanbevelingen gedaan voor de overheid om de privacy van haar burgers te waarborgen. Deze waarborgen verkleinen de handelingsruimte van de overheid echter niet, maar kunnen ter vergroting van de bescherming van de privacy en voornamelijk voor de beleving van de privacy worden ingezet. Denk hierbij aan bewustwording van gebruik van persoonsgegevens door de overheid en haar ambtenaren en bewustwording van burgers door uitleg over privacy wet- en regelgeving en voorlichtingsactiviteiten in het kader van de WBP, waardoor transparantie en voorspelbaarheid toenemen.
Specifieker is bijvoorbeeld een voorstel voor een differentiatie mogelijkheid waarbij een burger kan aangeven of hij al dan niet in aanmerking wil komen voor pro-actieve dienstverlening, een optie die binnen de kaders van de WBP kan worden ingevoerd. De aanbevelingen in de volgende paragraaf geven verdere opties voor de overheid, om binnen de grenzen van de WBP, om te gaan met privacy.

De tweede vraag ligt in het verlengde van de bovenstaande vraag. *Kan het handelingsvermogen van de overheid gelijk blijven of zelfs toenemen door een andere wijze van omgaan met persoonsgegevens?* Deze vraag kan bevestigend worden beantwoord.

De overheid in haar rol als dienstverlener kan door voorlichting te geven zowel haar handelingsruimte gelijk houden als de privacy(beleving) van haar burgers vergroten. Voor het vergroten van de handelingsruimte met inachtneming van de privacy zijn instrumenten als ‘ontkoppeld koppelen’ en een gedifferentieerd systeem voor pro-actieve dienstverlening geïntroduceerd.
In de democratische rol kan de overheid met inachtneming van de geschetste kanttekeningen doorgaan met het ontwikkelen van locatie-onafhankelijk stemmen.

In de rechtsstaat ligt de afweging moeilijker. Bij het omgaan met internet blijkt zelfregulering een zinvolle praktijk te zijn. Hierbij neemt de handelingsruimte van de overheid niet af en is de privacy voor rekening van de gebruikers. De Raad is voorstander van anonimiteit van de gebruiker op internet. Dit kan echter wel de handelingsruimte van de overheid verkleinen.
Bij *datamining* kan de WBP worden gevolgd, maar dient de overheid alert te blijven op de ruimte voor interpretatie die de WBP geeft. Bij wetgeving blijkt dat de Grondwet en de internationale- en nationale wetgeving aangepast dienen te worden aan de digitale samenleving. Omdat hierbij wordt uitgegaan van techniek-onafhankelijke beslissingen zal dit weinig consequenties voor de afweging handelingsruimte en privacy hebben. Dus zowel bij het aanpassen van de wetgeving als bij het omgaan met ICT-ontwikkelingen in de marktsector (zoals internet en *datamining*) kan in het algemeen aan het vergroten van het handelingsvermogen van de overheid en de privacybeleving van de burger tegelijkertijd worden voldaan.
Met name bij het opsporen en vervolgen van strafbare feiten is de afweging

tussen handelingsruimte en privacy problematisch. Hierbij betekent in veel gevallen een toename van het één, een afname van het ander. Anonimiteit op internet bijvoorbeeld, maakt opsporing en vervolging lastig. Ongelimiteerde cryptografie, bijvoorbeeld, leidt wel tot een toename van de privacy door grotere mogelijkheden voor beveiliging, maar ook tot een afnemend handelingsvermogen van de overheid inzake ontcijferen van berichten.

Concluderend geldt dus dat in de meeste gevallen door zorgvuldige omgang met persoonsgegevens zowel de handelingsruimte van de overheid als de privacy van de burger kan worden gewaarborgd. Kortom, als de overheid zich aan de voorwaarden voor rechtmatige verwerking van persoonsgegevens houdt, kan zowel het handelingsvermogen van de overheid als de privacy van de burgers afdoende worden beschermd.

Op de vraag *welke posities basisregistraties in de overheidsinformatie-huishouding hebben ten opzichte van sectorale indexen die zich ontwikkelen tot centrale registers met algemene gegevens*, is uitgebreid ingegaan in paragraaf 2.3. Kort samengevat is de Raad van mening dat het onderscheid tussen sectorale verwijsindices en centrale registers en het onderscheid tussen landelijke en decentrale registraties in het digitale tijdperk niet erg zinvol zijn. Hierbij geldt dat, veel meer dan de inrichting van de datahuishouding, zorgvuldigheid bij het omgaan met gegevens en zorgvuldigheid bij het toekennen van autorisaties van belang zijn. Voor een beschrijving van de overheidsinformatiehuishouding, de verschillende mogelijkheden hiervoor, en de voor- en nadelen van de verschillende methoden, wordt verwezen naar hoofdstuk twee van dit advies. De Raad is van mening dat in de nabije toekomst wellicht met intersectorale persoonsnummers en met unieke identificaties – met behulp van biometrie – zal worden gewerkt. De Raad vindt dit geen zorgwekkende ontwikkelingen en wijst wederom op het belang van zorgvuldigheid bij het omgaan met persoonsgegevens.

4.3
Aanbevelingen

Nieuwe digitale technieken en de angst voor een afnemend handelingsvermogen van de overheid hebben tot de adviesaanvraag geleid. Hoe kan in deze digitale samenleving de privacy van burgers worden gewaarborgd zonder dat de overheid buitenspel wordt gezet? Het antwoord hierop is de burger voorop te stellen en het gegeven dat privacy een recht van de burger is als vertrekpunt te nemen. Om te bereiken dat de overheid zowel haar burgers kan beschermen en diensten kan verlenen, en tegelijkertijd de privacy te waarborgen, worden de volgende instrumenten door de Raad aangereikt.

De volgende aanbevelingen betreffen instrumenten die de overheid kan toepassen om, in haar functioneren als dienstverlener in de verzorgingsstaat, zowel haar eigen activiteiten te ontplooien als rekening te houden met de privacy van de burgers.

De overheid dient voor een verantwoorde omgang met persoonsgegevens minimalistische gegevensverwerking als uitgangspunt te nemen.

In het kader van voorspelbaarheid en transparantie – dit zijn eisen die zowel burgers als de WBP aan het gebruik van persoonsgegevens stellen – stelt de Raad voor dat de overheid voorlichtingsactiviteiten over het gebruik van persoonsgegevens en privacy gaat ontwikkelen.

Een aanbeveling betreft het periodiek – bij voorkeur jaarlijks – verstrekken van een data-overzicht, waarbij iedere burger alle bij de overheid over hem of haar bekende informatie krijgt toegestuurd. Een goede informatiehuishouding kan op deze wijze 'schoon' blijven omdat burgers hun gegevens op juistheid kunnen toetsen en tegelijkertijd komt de overheid hiermee tegemoet aan de wens voor meer transparantie.

Voor pro-actieve dienstverlening wordt voorgesteld burgers een keuzemogelijkheid te geven. Burgers kunnen dan – net zoals bij direct-marketing activiteiten in de private sfeer – zelf aangeven wel of geen prijs te stellen op pro-actieve dienstverlening.
Bovenstaande aanbeveling betreft pro-actieve dienstverlening bij diensten die 'vrijwillig' zijn. Voor verplichte diensten, zoals het betalen van belasting, gaat informatievrijheid niet op. Bij verplichte diensten dient de overheid wel zorgvuldig om te gaan met persoonsgegevens en een minimaal gegevensbeheer te voeren, maar kan de burger niet zelf kiezen of hij zijn gegevens wil verstrekken. Deze mogelijkheid dient wel te worden gegeven bij de vrije diensten, zoals pro-actieve dienstverlening in het kader van de armoedebestrijding.

Met betrekking tot de inrichting van de informatiehuishouding van de overheid geeft de Raad de volgende aanbevelingen.
'Ontkoppeld koppelen', waarbij de ene administratie (vaak het sectoraal aanspreekpunt) aan de andere administratie doorgeeft wie aan gevraagde eisen voldoet, zonder daadwerkelijk gegevens door te geven, verdient de voorkeur boven andere vormen van het koppelen van gegevens.

Zorgvuldig toekennen van autorisaties is van groter belang dan de vraag of sectorale of centrale registraties de voorkeur verdienen. Dezelfde redenering geldt voor de vraag of de opslag van gegevens landelijk of decentraal moet geschieden.
Het toekennen van autorisaties dient met inachtneming van de in dit advies geschetste privacynormen en de voorschriften uit de WBP te geschieden.

Voor de informatiehuishouding is de Raad voorts van mening dat het principe van éénmalige opslag van gegevens een goed uitgangspunt is.
Hierbij dient de burger ook in kennis te worden gesteld van welke organisaties geautoriseerd zijn om in welke bestanden te 'kijken' en welke koppelingen van bestanden zijn toegestaan.

Er dient een grootschalige privacy-audit (door de Registratiekamer) te worden georganiseerd. Hierbij kunnen elektronische databestanden op elkaar worden afgestemd, kan de infrastructuur of de werking van de betreffende systemen worden geëvalueerd en kan de beveiliging van de systemen worden gecontroleerd en waar nodig worden versterkt.

Bij de overheid in haar democratische rol pleit de Raad voor elektronisch stemmen, maar wijst ook op de mogelijk nadelige gevolgen door de inrichting van het stembureau met behulp van de personal computer.
De Raad is van mening dat het ontwikkelen van elektronisch stemmen voorgezet dient te worden. Elektronisch stemmen biedt zowel een kans voor vergroting van de opkomst bij verkiezingen als voor een modern imago van de overheid. Er dient echter behalve voor de beveiliging van het anoniem stemmen ook rekening te worden gehouden met beïnvloeding op het virtuele stembureau en het ronselen van stemmen. Deze laatste twee voorbehouden dienen voordat het elektronisch stemmen in werking treedt, te zijn opgelost.

Bij de eerste paar verkiezingen na het invoeren van elektronisch stemmen dient zowel elektronisch stemmen als het stemmen op de traditionele stembureaus mogelijk te zijn.

Bij het laatste thema – 'ICT en privacy' in de rechtsstaat – is het ontwikkelen van goede beleidsvoornemens moeilijker. In tegenstelling tot de rol van de overheid in de verzorgingsstaat zijn er in de rechtsstaat bij de afweging tussen 'ICT en privacy' soms geen win-win situaties. De Raad beveelt daarom aan een goede tussenweg te zoeken tussen zelfregulering en regulering door de overheid. De volgende instrumenten zijn hiervoor handreikingen.

Veiligheid (privacy) van communicatie en transacties via internet dienen primair voor rekening te komen van gebruikers en aanbieders op het net. Eigen verantwoordelijkheid, het recht op anonimiteit op internet en marktwerking staan centraal.

Ongerechtvaardigd gebruik van persoonsgegevens en het verwerken van vervuilde bestanden dient te worden bestraft. Privacyschending dient te worden beboet. Dit kan zowel door strafrechtelijk optreden als door het invoeren van schade-vergoedingen geschieden. Pas als privacyschending niet langer kosteloos is, zal een zorgvuldige omgang met persoonsgegevens kunnen worden gewaarborgd.

Voor het maken van profielen, onder andere door *datamining*, zijn ook voorschriften in de WBP opgesteld. Mogelijke nadelige consequenties van de profielen zijn uitsluiting, risicoselectie en *informatiestalking*. Om de risico's van het creëren van profielen te beperken is in de WBP het artikel over 'het recht op menselijke tussenkomst' opgenomen. Hierin staat dat niet uitsluitend op grond van geautomatiseerde gegevensverwerking beslissingen mogen

worden genomen die de betrokkene in aanzienlijke mate treffen. *Informatiestalking* valt hier niet onder, maar het is wel een ontwikkeling waar burgers bezorgd over zijn. Daarom heeft de Raad de volgende aanbeveling opgesteld.
Het verdient aanbeveling een jaarlijkse mailing te organiseren waarin de adressen staan van organisaties die voor marketingdoeleinden Naam, Adres, Woonplaats en Telefoonnummer(NAWT)- bestanden doorverkopen (zoals DMSA en KPN). In deze mailing dient de mogelijkheid te worden geboden, door middel van een antwoordkaartje, aan te geven geen prijs te stellen op telefonische of schriftelijke colportage.

De Raad ondersteunt de actualisering van de wetgeving (Grondwet, Internationaal recht, WBP, Strafrecht) in het digitale tijdperk. Hierbij dient te worden gezocht naar zoveel mogelijk techniek-onafhankelijke wetgeving.

Over het versleutelen – geheim maken – van gegevensverkeer over internet heeft de Raad de volgende mening: *De bovengrens van 512 bits op het versleutelen van berichten en transacties – de bovengrens op cryptografie – dient te worden opgeheven. Digitaal verkeer wordt daardoor veiliger.*

Geraadpleegde literatuur

- Artz, M.(1999) 'Profilering en privacy; nieuwe privacywetgeving biedt mogelijkheden voor datawarehousing en datamining'. In: *Informatie en Informatiebeleid,* nr. 1.
- Borking, J.; Artz, M. en Almelo, L. van (1998) *Gouden bergen van gegevens. Registratiekamer*: Achtergrondstudies en Verkenningen, nr. 10.
- Bovens, M. A. P. (1999) *De digitale rechtsstaat; beschouwingen over informatiemaatschappij en rechtsstaat*. Alphen aan den Rijn: Samsom.
- Buurman, M. (1999) 'De toekomst van Internet stemmen'. In: *Nieuwe media Burger en Bestuur*, nr. 5, Instituut voor Publiek en Politiek.
- Commissie Grondrechten in het digitale tijdperk (1999) *Vraagpunten inzake grondrechten in het digitale tijdperk*. www.minbzk.nl/gdt.
- Eck, B.M.A. van (1999) 'Van voor naar achter, van links naar rechts; niet de cliënten, maar hun gegevens gaan rond'. In: *Privacy en Informatie*, nr. 5.
- EK 25 892, nr. 92. *Regels inzake de bescherming van persoonsgegevens* (Wet bescherming persoonsgegevens), 1999-2000.
- Engelberts, J. (1999) 'Big Brother niet alleen maar op TV'. In: *Metro*, 21 december 1999.
- EPN (1999) EPN-dossier *veiligheid op internet*. www.epn.net/actueel/1999.
- Gemeente en privacy (I & II). In: *Handboek Privacy*, 5 maart 1999.
- Gunsteren, H.R. van (1994) *Culturen van besturen*. Amsterdam: Boom.
- Gutwirth, S. (1998) 'Privacy vrijheid versus verwerking van persoonsgegevens'. In: *Privacy geregistreerd; visies op de maatschappelijke betekenis van privacy*. Den Haag: Rathenau Instituut.
- Hamelink, C.J. (1999) *Digitaal Fatsoen; mensenrechten in cyberspace*. Amsterdam: Boom.
- Holsheimer, M. (1999) 'Datamining ontdekt waardevolle informatie in databases'. In: *Privacy en Informatie*, vol 2, nr. 3.
- Holvast, J. (1999) 'Oude bergen in een nieuw landschap'. In: *Privacy en Informatie*, vol 2, nr. 3, p. 105-109.
- Koops, B-J. (1997) 'Een richtlijn zonder richting'. In: *IT & Recht*, nr. 3, p.1-3.
- Lohman, F.A.B. (1999) *The Effectiveness of Management Information; a design approach to contribute to organizational control*. Amsterdam: Thela Thesis.
- Minister De Vries in: 'Cliënt-volgsysteem vergt bestuurlijke aanpassingen'. *VNG-magazine*, 26 november 1999, p. 9.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (1999). Rapport: *Voorbij het loket*.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (1999). Rapport: *Bewegingen in het bestuur*. Hoofdstuk 2; Naar een betere dienstverlening.
- Mutsaers, L. (1998) 'De Gemeentelijke Basisadministratie; verleden, heden en toekomst'. In: *Privacy en Informatie*, nr. 3.
- Nouwt, S. en Voermans, W. (red.) (1996) *Privacy in het informatietijdperk*. Den Haag: Sdu.

- OECD privacy richtlijn. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. www.oecd.org.
- Raad voor het openbaar bestuur (1999) *Het bestuurlijk kraakbeen*. Den Haag, december 1999.
- Rathenau Instituut (1998) *Privacy geregistreerd: Visies op de maatschappelijke betekenis van privacy*. Amsterdam: Cramwinkel.
- Rathenau Instituut (1998) *Privacy vrijheid!: De vrijheid om zichzelf te zijn*. Amsterdam: Cramwinkel.
- Registratiekamer (1998) 'Encryptie niet aan banden leggen'. In: *Privacy en Informatie*, nr. 2.
- Riker, W.H. (1988) *Liberalism Against Populism; A confrontation between the theory of democracy and the theory of social choice*. Illinois: Waveland Press.
- Ruiter, de A. (1998) 'Problematische privacy'. In: *Privacy geregistreerd; visies op de maatschappelijke betekenis van privacy*, p. 287. Den Haag: Rathenau Instituut.
- Smink, G.C.J.; Haamstra, A.M. en Dijk, H.M.L. van (1999). *Privacybeleving van burgers in de informatiemaatschappij*. Den Haag: Rathenau Instituut.
- Staatscourant (1999) *Belastingdienst springt niet zorgvuldig om met privacy*, 11-11-1999, nr. 218.
- Stichting Maatschappij, Veiligheid en Politie (1999) *Fraude en het Internet en het achtergrondrapport*.
- Stichting Maatschappij, Veiligheid en Politie (1999) *Achtergronden van Internetfraude*.
- Stol, W.; Treeck, R. van en Ven, S. van der (1999) 'Criminaliteit met informatie- en communicatietechnologie; politie in een nieuwe sociale context'. In: *Tijdschrift voor Criminologie*, vol 41, nr. 4.
- Tjeenk-Willink, H.D. (1999) '*Als de overheid niet alles kan, wat moet ze dan*?' In: Staatscourant, nr. 184, 24 september 1999.
- TK 26 387, nr. 1. *Actieprogramma Elektronische Overheid*. Handelingen Tweede Kamer, 1998-1999
- TK 25 880, nr. 1-2. *Wetgeving voor de elektronische snelweg*. Handelingen Tweede Kamer, 1998-1999
- Tops, P. (1999) 'De esthetiek van het stemmen'. In: *nieuwe media Burger en Bestuur*, nr. 5, november 1999. Instituut voor Publiek en Politiek.
- Wetenschappelijke Raad voor het Regeringsbeleid (1998) *Staat zonder Land*. Den Haag: Sdu.
- Zuurmond, A. e.a.(1998). Preadvies Rob. *Dienstverlening centraal, de uitdaging van ICT voor de publieke dienstverlening*.
- Zuurmond, A. e.a. (red) (1994) *Informatisering in het openbaar bestuur*. Den Haag: VUGA.

Bijlage I

Adviesaanvraag

Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Aan
de voorzitter en leden van de Raad voor het openbaar bestuur,
Kalvermarkt 53,
Den Haag

Bijlagen	Uw kenmerk	Ons kenmerk	Datum
		DIOS/DT99/U82599	14 september 1999
Inlichtingen bij		Doorkiesnummer	
J.W. Flier		0703026122	
Onderwerp		Departementsonderdeel	
adviesaanvraag ICT en privacy		DGOB/DIOS/D&T	

In het werkprogramma 1999 van de Raad is op mijn verzoek opgenomen dat een advies zal worden uitgebracht over het onderwerp ICT en privacy. Ter concretisering hiervan kom ik hierbij tot een formele adviesaanvraag.

In het advies 'Staat zonder land' concludeert de WRR dat de stormachtige ontwikkeling van de informatie- en communicatietechnologie (ICT) een afnemende binding aan een bepaald grondgebied (deterritorialisering) tot gevolg heeft met onvermijdelijke gevolgen voor het handelingsvermogen van de staat. De WRR concludeert dat dit handelingsvermogen in beginsel zal afnemen. Er zijn echter ook mogelijkheden om door beter in te spelen op externe veranderingen weer handelingsvermogen te herwinnen, bijvoorbeeld door het zelf benutten van de mogelijkheden van ICT.

De WRR wijst er op dat in de recente bestuurskundige en juridische literatuur vooral het versterkt instrumenteel vermogen van de staat in het brandpunt staat: '*ICT maakt een betere publieke dienstverlening op maat mogelijk, maar dit vraagt anderzijds ook om een toenemende registratie van gegevens en controle op de gegevens die de burgers aanreiken. De koppeling van verschillende databestanden kan ook worden gebruikt voor verbetering van de algemene beleidsvorming, waarbij maatschappelijke situaties, zoals sociale achterstanden, vooraf zo scherp mogelijk in beeld worden gebracht, bijvoorbeeld als basis voor de verdeling van welzijnsubsidies. Aldus wordt de burger steeds gedetailleerder in kaart gebracht. Verhoogde beleidsambities om nog gerichter te interveniëren en nog meer dienstverlening op maat te bieden, botsen dan in toenemende mate met beginselen zoals privacy*' (p. 75).

De WRR concludeert dan ook dat de inwerking van ICT ambigu is: '*Dezelfde technologische ontwikkelingen die de externe doeltreffendheid van het handelen van de staat doen afnemen, kunnen op onderdelen de doelmatigheid van bepaalde beleidsinstrumenten vergroten*' (p. 78).

Postadres
Postbus 20011
2500 EA Den Haag

Telefoon (070) 302 63 02
Telefax (070) 363 91 53

Bezoekadres
Schedeldoekshaven 200
2511 EZ Den Haag

Verzoeke bij beantwoording datum, kenmerk en onderwerp te vermelden

Of en zo ja hoeveel de staat aan handelingsvermogen zal inboeten lijkt hiermee mede in belangrijke mate bepaald te gaan worden door de vraag hoe ICT zal worden ingezet en hoe er om zal worden gegaan met het vraagstuk van de privacy van persoonsgegevens.

Naast deze algemene vraagstelling is ook een specifiek voorbeeld van de mogelijkheden van ICT en gegevensuitwisseling aan de orde namelijk de inrichting van een informatiehuishouding op macro-niveau. Op dit moment bestaan er wat dat betreft voornamelijk twee concepten, te weten: het concept van basisregistraties en het concept van sectorale verwijsindexen. Deze beide concepten vullen elkaar over het algemeen goed aan.

Bij basisregistraties gaat het in beginsel om landelijke authentieke gegevensbronnen, waarin op gestandaardiseerde manier gegevens zijn vastgelegd en waaruit op brede schaal verstrekkingen plaatsvinden met behulp van gestandaardiseerde uitwisselingsformaten. Voorbeelden van basisregistraties zijn de GBA voor algemene persoonsgegevens en de belastingdienst voor o.m. inkomensgegevens. De gedachte achter dergelijke basisregistraties is dat gegevensopslag op meer dan één plek onnodig wordt. Sectorale verwijsindexen zorgen voor standaardisatie en stroomlijning van gegevensstromen binnen een sector. De sectoren richten verwijsindexen in, waarin wordt vastgelegd welke organisatie welke gegevens bijhoudt. Dit maakt het voor organisaties binnen en buiten de sector mogelijk om vast te stellen bij wie nadere informatie kan worden gevraagd. Het concept van centrale verwijsindexen is sterk in opkomst.

Bij het inrichten van sectorale verwijsindexen kan een tendens worden waargenomen dat de sectorale index meer dan alleen verwijsgegevens gaat bevatten. Die ontwikkeling zet het concept van basisregistraties onder druk en heeft effect op de privacybescherming die vanuit de basisregistratie gezien kan worden geboden. De uit een authentieke bron aan een sectoraal bestand verstrekte gegevens worden uit dit bestand weer verstrekt aan de verschillende uitvoerende onderdelen. Daardoor worden de mogelijkheden voor de authentieke bron kleiner om de omvang van de gegevensverstrekking aan de sectorale onderdelen te bepalen.

Naar aanleiding hiervan vraag ik de Raad graag advies over de volgende vragen:

- Welke verschillende opties bestaan er in dit licht voor de overheid om binnen het kader van de toekomstige Wet bescherming persoonsgegevens in het algemeen om te gaan met het privacy-begrip (bijv. m.b.t. persoonsnummers) en wat betekent dit voor het handelingsvermogen van de overheid?
- Betekent meer handelingsvermogen vanzelf minder privacy of zijn er ook mogelijkheden om door een andere wijze van omgaan met persoonsgegevens meer handelingsvermogen te realiseren met evenveel of zelfs meer privacy?
- Welke positie hebben basisregistraties in de overheidsinformatiehuishouding ten opzichte van sectorale indexen die zich ontwikkelen tot centrale registers met algemene gegevens?

Hoogachtend,
DE MINISTER VOOR GROTE STEDEN- EN INTEGRATIEBELEID

R.H.L.M. van Boxtel

Bijlage II

Overzicht van uitgebrachte adviezen

• ICT en het recht om anoniem te zijn	januari 2000
• Op het toneel en achter de coulissen, de regiefunctie van gemeenten	december 1999
• Samen werken aan veiligheid, de bestuurlijke inbedding van de veiligheidsregio's	december 1999
• Het bestuurlijk kraakbeen	december 1999
• Bijzondere opsporingsdiensten	juni 1999
• Retoriek en realiteit van het integratiebeleid	maart 1999
• Kiezen zonder drempel, het kiesstelsel geactualiseerd	februari 1999
• De grenzen van de Internetdemocratie	december 1998
• De overheid de markt in- of uitprijzen?	december 1998
• Tussen staat en electoraat; politieke partijen op het snijvlak van overheid en samenleving	september 1998
• Wijken of herijken: nationaal bestuur en recht onder Europese invloed	september 1998
• Illegale Blijvers	april 1998
• Bestuurlijke betrekkingen tussen kabinet, VNG en IPO	april 1998
• Op de handhaving beschouwd; toezien op een versterkte en uitvoerbare lokale handhavingsstructuur	april 1998
• Dienen en verdienen met ICT; over de toekomstige mogelijkheden van de publieke dienstverlening	april 1998
• Op de grens van monisme en dualisme	november 1997
• Integriteit, een zaak van overheid èn bedrijfsleven	oktober 1997
• Verscheidenheid in vervlechting; bestuurlijke instrumenten tussen proces en institutie	oktober 1997

Bijlage III

Overzicht van uitgebrachte preadviezen en overige publicaties

Preadviezen

1. D.M. Berkhout e.a., *De provincie in het vizier, opstellen over het Nederlandse middenbestuur*	december 1999
2. S.A.H. Denters e.a., *De regiefunctie in gemeenten*	december 1999
3. L.F.M. Besselink en R.J.G.M. Widdershoven, *De juridische gevolgen van Europese integratie voor het nationaal beleid*	september 1998
4. A. Zuurmond e.a., *Dienstverlening centraal, de uitdaging van ICT voor de publieke dienstverlening*	april 1998
5. O.J.D.M.L. Jansen, *Bestuursrechtelijke en strafrechtelijke handhaving, bestuur en politie*	januari 1998

Overige publicaties

1. Werkprogramma 2000	september 1999
2. Jaarverslag 1998	maart 1999
3. Werkprogramma 1999	september 1998
4. Verslag symposium, *De gezondheidstoestand van het Nederlandse openbaar bestuur*; Ziek of gezond	maart 1998
5. Jaarverslag 1997	maart 1998
6. Verslag studiemiddag, *Sturingsinstrumenten en hun context. De modernisering van het bestuursintrumentarium bij (financiële) decentralisatie*	september 1997
7. Werkprogramma 1998	september 1997

Bijlage IV

Samenstelling Raad voor het openbaar bestuur

voorzitter	:	de heer **mr. H.J.E. Bruins Slot**, hoofddirecteur Informatie Beheer Groep;
vice-voorzitter	:	de heer **prof.dr. H.G. Sol**, hoogleraar systeemkunde aan de Technische Universiteit Delft;
leden	:	de heer **prof.dr. H.B. Entzinger**, hoogleraar algemene sociale wetenschappen aan de Universiteit Utrecht;
	:	mevrouw **mr. W.L. Gillis-Burleson**, directeur Legato opleidingen;
	:	de heer **prof.mr. P.F. van der Heijden**, hoogleraar arbeidsrecht aan de Universiteit van Amsterdam;
	:	de heer **drs. P.J. Langenberg**, hoofd afdeling Strategie & Beleid dIVV, gemeente Amsterdam
	:	de heer **drs. P.A. Lankhorst**, adviseur Jeugdbeleid en Jeugdzorg,
	:	de heer **ing. E.M. Mastenbroek**, oud-commissaris van de Koningin in de provincie Limburg;
	:	mevrouw **G.W. van Montfrans-Hartman**, associée BCG;
	:	mevrouw **A.G.M. van de Vondervoort**, senior adviseur bij Bakkenist Management Consultants
	:	de heer **prof.dr. C.D. van der Vijver**, directeur Stichting Maatschappij, Veiligheid en Politie;
secretaris	:	de heer **drs. M.P.H. van Haeften** (geen Raadslid).

Bijlage V

Participanten expertmeeting 'ICT en privacy'
18 oktober 1999 te Den Haag

De heer P. Dieleman (Roccade Public, Apeldoorn)
De heer dr. J. A. G. M. van Dijk (Vakgroep Massacommunicatie, Universiteit Utrecht)
De heer drs. J. G.W. van der Flier (Ministerie Justitie, Den Haag)
De heer J. van Heeswijk (Elite Mail, Uden)
Mevrouw drs. J. A. M. van Hilgersom (Hoofd Sociale Dienst, Gemeente Den Haag)
De heer drs. S. L. Lelieveldt (De Nederlandsche Bank, Amsterdam)
De heer dr. U. van der Pol (Registratiekamer, Den Haag)
De heer G. van Rossum (Origin, Leidschendam)
De heer mr. E. Schreuders (Centrum voor Recht, Bestuur en Informatisering, KUB, Tilburg)
Mevrouw drs. C. L. M. de Vries (ING bank, afd. Direct Marketing, Diemen)
De heer dr. A. Zuurmond (Roccade Civility, Rotterdam)