R e g i s t r a t i e k a m e r

Vaste Commissie voor Justitie
uit de Tweede Kamer der Staten-Generaal

's-Gravenhage, 1 september 1998
Ons kenmerk 98.A.0711.02
Onderwerp Wetgeving voor de elektronische snelweg (25 880)

Op het eerste gezicht kan de nota Wetgeving voor de elektronische snelweg (WES)(Kamerstukken II, 1997-1998, 25 880, nrs. 1-2) worden aangemerkt als een brede verkenning van het verschijnsel elektronische snelweg met daarin een goede en evenwichtige aanzet voor normvorming, ook op het terrein van de bescherming van de privacy. Met het oog op de parlementaire behandeling van de nota plaatst de Registratiekamer echter enkele kanttekeningen bij de nota en de daarin vervatte beleidsvoornemens. Zij laat zich hierbij leiden door haar eigen ervaringen op het onderhavige terrein en constateert voorts dat recente ontwikkelingen, bijvoorbeeld met betrekking tot de Telecommunicatiewet en encryptie daarmee niet steeds sporen. In dit bestek volstaat de Registratiekamer met het plaatsen van kanttekeningen bij de volgende onderwerpen:

1. Het normatieve uitgangspunt dat wat off-line geldt ook on-line moet gelden;
2. Het risico dat technische faciliteiten de juridische norm bepalen;
3. De gevolgen van datamining;
4. De vervaging van bestaande onderscheidingen in elektronische communicatie;
5. De wisselende opstellingen van het kabinet ten aanzien van encryptie.

1. Off-line/on-line

Met betrekking tot de elektronische snelweg benadrukt het kabinet de ordenende functie van de overheid. Het faciliteren van de elektronische snelweg kan slechts plaatsvinden onder waarborging van fundamentele waarden en normen. Het uitgangspunt wordt

Uw brief
Bijlagen
Contactpersoon
Doorkiesnummer

Prins Clauslaan 20
Postbus 93374
2509 AJ 's-Gravenhage
Tel. 070-3811300
Fax 070-3811301

gehanteerd dat wat "off-line" geldt ook "on-line" moet gelden, d.w.z. dat op de elektronische snelweg in beginsel dezelfde normen worden gehanteerd als daarbuiten. Dit uitgangspunt geldt zowel voor de bescherming van burgers als voor de bevoegdheden van de overheid.

De beschermingsfunctie ten opzichte van de burgers krijgt een extra dimensie op de elektronische snelweg. In de nota wordt opgemerkt: "In het gewone maatschappelijke verkeer kunnen burgers zich in beginsel anoniem op de openbare weg bewegen. Het vragen naar de identiteit is voorbehouden aan personen die daartoe op grond van de wet zijn bevoegd. (…) De realiteit op de elektronische snelweg is dat deelnemers daaraan altijd persoonsgegevens achterlaten die op enigerlei wijze inzicht geven in hun persoon. (…) De elektronische snelweg vergroot zowel de behoefte aan een meer persoonsgebonden identiteitsvaststelling, als aan anoniem deelnemen aan het elektronisch verkeer." (blz. 129) Uitgangspunt dient echter te zijn dat waar geen wettelijke noodzaak tot identificatie bestaat anonieme deelname aan de elektronische snelweg mogelijk moet zijn. De Registratiekamer onderschrijft dit uitgangspunt van harte. Ook in het verband van de Europese privacybescherming is het uitgangspunt aanvaard van "anonimity on internet". Dit uitgangspunt is onder meer verwoord door de Werkgroep als bedoeld in art. 29 van Richtlijn nr. 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Pb EG/L281/31), een permanente werkgroep waarin de nationale toezichthouders van de lidstaten van de Europese Unie zitting hebben. In een hieraan gewijd document neemt de werkgroep het standpunt in dat "the ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on line as they currently enjoy off-line" (Recommendation 3/97 van 3 december 1997).

Voor het kabinet vormt de aan het gebruik van de elektronische snelweg inherente beperking van de mogelijkheden voor afscherming van de gebruiker aanleiding om de inzet van "privacy-enhancing technologies" (PET) te bevorderen (blz. 130). Dit beleidsvoornemen is geheel in overeenstemming met de visie van de Registratiekamer, die is neergelegd in haar rapport "Privacy-enhancing technologies: the path to anonimity" dat zij in 1995 samen met haar Canadese zusterorganisatie heeft uitgebracht (serie Achtergrondstudies en Verkenningen 5A en 5B). Van belang is dat gezien het

mondiale karakter van de elektronische snelweg, PET als ontwerpbeginsel m.b.t. informatiesystemen en bijvoorbeeld intelligente software agents mondiaal wordt gepropageerd.

Helaas dingt het kabinet ook direct weer af op het gebruik van PET-methoden. Het kabinet stelt dat om geen afbreuk te doen aan de taak en mogelijkheden van opsporende en toezichthoudende instanties of aan het belang van de veiligheid van de staat, het van groot belang is dat er bij toepassing van PET altijd een mogelijkheid aanwezig is om de gegevens naar personen te herleiden. Het kabinet noemt deze belangen van een hogere orde dan de bescherming van de privacy (blz. 133).
Dit uitgangspunt wordt uitgewerkt in twee scenario's:

- Ten behoeve van het opsporingsbelang kan niet langer meer worden vastgehouden aan het uitgangspunt dat burgers anoniem aan de elektronische snelweg moeten kunnen deelnemen. Met andere woorden: burgers moeten accepteren dat hun identiteit in verband met het daarmee gediende opsporingsbelang altijd bij één van de actoren op de elektronische snelweg bekend is.
- Identificatie en registratie bij het betreden van de elektronische snelweg vormt een te grote inbreuk op het recht van privacy. Ten behoeve van de opsporing moet worden gezocht naar alternatieven voor registratie die een minder vergaande inbreuk op de privacy opleveren. Dit kan leiden tot een bijstelling van het ambitieniveau bij de opsporing op de elektronische snelweg." (blz. 162)

Een duidelijke keuze maakt het kabinet - nog - niet. Wel wordt opgemerkt dat het scenario waarbij te allen tijde identificatie en registratie is vereist op voorhand niet aantrekkelijk lijkt . Dit is zwak uitgedrukt en naar de mening van de Registratiekamer een veel te halfslachtige stellingname. Een keuze voor het eerste scenario is nu juist onaanvaardbaar in het licht van het uitgangspunt dat de off-line geldende kaders ook on-line maatgevend zijn. Hierin past geen keuze voor een permanente identificatie- en registratieverplichting. Voor dergelijke vergaande maatregelen is ook geen klemmende noodzaak aanwezig. In zijn preadvies voor de jaarvergadering van de Nederlandse Juristenvereniging, die dit jaar was gewijd aan Recht en Internet, merkte prof. mr. A.W Koers in dit verband op dat niet langer de bedreiging wordt gevormd doordat Internet immuniteit aan criminelen lijkt te bieden. Hij noemt dit een misverstand en waarschuwt voor een andere ontwikkeling: "Met het groter worden van de ervaring van

opsporingsambtenaren begint duidelijk te worden dat Internet misschien wel betere mogelijkheden biedt voor het opsporen van strafbare feiten dan oorspronkelijk gedacht". Diverse beleidsvoornemens in deze nota wijzen in deze richting en het is ook de ervaring van de Registratiekamer dat de aktiviteiten om grip te krijgen op elektronische communicatie nog lang niet zijn uitgeput. Dit betekent niet dat deze vorm van communicatie geen bijzondere normering behoeft, zowel ten aanzien van de rechtsbescherming als de bevoegdheden om hierop inbreuk te maken. Een goed voorbeeld hiervan is de erkenning van het "briefgeheim" ten aanzien van e-mail. Een logisch gevolg hiervan is dat een wettelijke mogelijkheid wordt geschapen om op een wijze die in overeenstemming is met artikel 8 EVRM t.b.v. de opsporing van strafbare feiten of de veiligheid van de staat hierop een inbreuk te maken. Een dergelijke aanpak kan als evenwichtig worden geschetst ten aanzien van vragen die nieuwe vormen van communicatie genereren.

2. Technische faciliteiten en legitimatie

Het is van alle tijd dat de techniek voorloopt op de juridische normontwikkeling. Terecht wordt dan ook in de nota het gevaar onderkend dat de technische mogelijkheden van de elektronische snelweg tot maatstaf worden voor hetgeen maatschappelijk als geoorloofd gebruik wordt beschouwd. Het is de ervaring van de Registratiekamer hierbij dat ofwel te gemakkelijk de technische mogelijkheden de juridische normen definiëren, ofwel een gapende kloof ontstaat tussen de door de techniek gedomineerde praktijk en het juridisch kader. Als voorbeelden wijst zij op het gemak waarmee in een fase waarin de juridische status van e-mail nog onduidelijk was, binnen (overheids)organisaties deze post van medewerkers werd gecontroleerd. Het ging om een werkwijze die overeenkwam met het openbreken van bureauladen van medewerkers, waartoe de gemiddelde werkgever onder vergelijkbare omstandigheden niet of veel selectiever zou overgaan. Hetzelfde geldt voor het vastleggen van telefoongesprekken in digitale (huis)telefooncentrales. Het enkele feit dat dit technisch eenvoudig te verwezenlijken is brengt beheeerders ertoe hiertoe over te gaan. Deze ontwikkeling wordt gestimuleerd door de zoekmethoden, zoals datamining, met behulp waarvan in een brei van bits en bytes relevante informatie kan worden opgespoord. Uitgangspunten voor een zorgvuldig gebruik van deze informatie zijn te vinden in het

rapport van de Registratiekamer “Als de telefoon wordt opgenomen”, november 1996. De beginselen van proportionaliteit en subsidiariteit dienen hierbij richtinggevend te zijn evenals de waarborgen en de transparantie waarmee het gebruik van dergelijke gegevens binnen een organisatie is omgeven. Dit geldt in versterkte mate voor situaties waarin de overheid, anders dan als werkgeefster optreedt als publiekrechtelijke macht. De inbreuk die zij dan maakt dient een wettelijke grondslag te hebben en ook overigens in overstemming te zijn met de vereisten die hieraan ingevolge artikel 8 EVRM zijn verbonden.

3. Datamining

Technische mogelijkheden kunnen zulke ingrijpende gevolgen hebben voor de verwerking en het gebruik van persoonsgegevens dat compenserende juridische normering noodzakelijk is. Dit geldt met name voor de zoek- en analysemethode datamining. Ook in de nota worden de bijzonder ingrijpende mogelijkheden van datamining onderkend. Een voorbeeld van de aanwending hiervan vormt het voornemen om dienstverleners op de elektronische snelweg, zoals internet service providers (ISP) te verplichten - ten behoeve van de opsporing van strafbare feiten - bij te houden (loggen) welke handelingen (al dan niet verdachte) abonnees op de elektronische snelweg uitvoeren.
Dit kan een eerste stap zijn op weg naar vergaande inbreuken op de bescherming van de privacy van alle gebruikers van de snelweg. Het is goed hierbij te bedenken dat een ISP zeer veel gegevens kan registreren van gebruikers, die niet alle noodzakelijk zijn of slechts voor een beperkte tijd voor de bedrijfsvoering. Zo kunnen in principe ISP’s logs bijhouden van het tijdstip en de plaats van het inloggen, de tijdsduur, de deelname aan usenetgroepen en de geposte berichten, de opgehaalde software van een site of usernetgroup, de gevoerde gesprekken via internettelefonie en de videoconferences die zijn gehouden, de verzonden e-mails en hoe vaak de postbus is geraadpleegd, de bezochte websites en de interactie tussen de gebruiker en de site, het bestellen van produkten via een Internetside. Deze opsomming is niet uitputtend.

Deze set gegevens geeft een aanzienlijke hoeveelheid informatie over de betreffende abonnee. Uit deze informatie kunnen opsporingsinstanties, maar ook andere organisaties

of personen achteraf een zeer gedetailleerd beeld vormen van een persoon en ook op voorhand abonnees profileren. Het is duidelijk dat dergelijke onderzoeken tengevolge van de vergaande zoek- en analysemethoden van datamining zeer ingrijpend kunnen zijn voor de hieraan onderworpen burgers. Bij gebruik door opsporingsinstanties en veiligheidsdiensten kan het hierbij gaan om burgers ten aanzien van wie nog niet enige verdenking bestaat van het betrokken zijn bij een strafbaar feit of het in gevaar brengen van de veiligheid van de staat.

In het algemeen dient de regulering van het gebruik van datamining naar de opvatting van het kabinet te geschieden via de eisen die aan het (on)verenigbaar gebruik van persoonsgegevens worden gesteld ingevolge de nieuwe Wet bescherming persoonsgegevens. De Registratiekamer verwacht evenwel dat deze benadering geen toereikende besccherming zal bieden. Een dwingende combinatie is noodzakelijk van technologie en recht om een adequaat niveau van privacybescherming te kunnen realiseren. Dit vergt een technische inrichting van een informatiesysteem die zorgvuldig is afgestemd op de specifieke gebruiksvoorschriften. De Registratiekamer komt binnenkort met een rapport over dit onderwerp uit waarin de juridische aspecten van de technieken van datamining en datawarehousing worden geschetst.

Datamining vormt een goede illustratie van de noodzaak van wetgeving ten aanzien van de bescherming van persoonsgegevens in het algemeen. In recente kritiek van onder meer VNO/NCW en de Consumentenbond ten aanzien van de bij uw Kamer voorliggende Wet bescherming persoonsgegevens is een pleidooi gehouden voor meer vertrouwen in de zelfbeschikking van de mondige burger, wat de voorgenomen informatieplicht van bedrijven en organisaties overbodig zou maken. De Registratiekamer acht deze opstelling een overschatting van diens mogelijkheden die de effectiviteit van de beoogde bescherming slechts kan ondergraven. De draagwijdte van het gebruik van technieken als datamining ontgaat de gemiddelde burger van wie in het kader van deze technieken wel profielen worden ontwikkeld, op grond waarvan vervolgens beslissingen over hem worden genomen. Verplichtingen, zoals in het wetsvoorstel zijn vervat, om dergelijke praktijken transpararant te doen zijn en van andere structurele waarborgen te voorzien, vormen toch wel een minimum garantie voor een toereikende bescherming van de burgers.

De Registratiekamer onderschrijft het standpunt van het kabinet dat voor het gebruik van datamining als opsporingsmethode een degelijke basis dient te worden gelegd in het Wetboek van Strafvordering. Dit betekent dat het gebruik door opsporingsinstanties slechts kan plaatsvinden in situaties waarin strafvorderlijk optreden geindiceerd is. Aparte aandacht verdient de vraag of en in welke mate de overheid aanbieders van diensten mag verplichten ten behoeve van een potentieel opsporingsbelang of belang van de staatsveiligheid gegevens vast te leggen of te genereren die niet noodzakelijk zijn voor de eigen bedrijfsvoering. Een kwalijk precedent is in de ogen van de Registratiekamer geschapen door de aanvaarding van artikel 13.4 van de Telecommunicatiewet door uw Kamer (zie nader onder 4).

4. Vervaging bestaande onderscheidingen

In de Nota WES wordt terecht onderkend dat anders dan bij analoge technieken in de digitale wereld geen goed onderscheid meer kan worden gemaakt tussen opslag en transport van informatie. Het kabinet verbindt daar evenwel (nog) geen gevolgen aan. Op losse gronden wordt aangenomen dat de wetgever dit onderscheid wel kan blijven hanteren. Het onderscheidend criterium is in de visie van het kabinet of een gegeven valt te raadplegen op een door de mens te bepalen tijdstip. Deze benadering overtuigt de Registratiekamer niet. Een telefoongesprek kon altijd al gedurende het transport worden afgeluisterd dan wel worden opgenomen op een gegevensdrager. De veronderstelling dat daarbij geen sprake is van raadpleging op een door de mens te bepalen tijdstip is eenvoudig onjuist. Ten aanzien van de digitale elektronische informatie- en communicatienetwerken moet worden geconstateerd dat gegevens(bestanden) in snel wisselende toestanden van transport of opslag kunnen verkeren of zelfs in beide toestanden tegelijk. Het ontgaat de Registratiekamer om welke redenen de gegevens die bij het transport tijdelijk worden opgeslagen niet zouden zijn te raadplegen (zie blz. 22). Onderscheppingen tijdens het transport zijn daarmee steeds minder te onderscheiden van het achterhalen van opgeslagen informatie. Ook vervaagt het onderscheid tussen computers en telecommunicatienetwerken steeds verder. Het is daarbij de vraag of het onderscheid tussen computerhuiszoeking en het tappen van telecommunicatienetwerken nog wel zinvol is. De Registratiekamer heeft hierop ook gewezen in haar advies over het concept-wetsvoorstel Computercriminaliteit (29 maart 1997, nr. 98.A.089.01).

Bijzondere aandacht hierbij verdient de omstandigheid dat de rechtsbescherming en de bevoegdheden om inbreuken te maken nu beperkt zijn tot openbare netwerken. In de Telecommunicatiewet is dit probleem zichtbaar geworden doordat nota bene aan de Minister van Verkeer en Waterstaat de bevoegdheid is toegekend om te beslissen over het onderscheppen van de communicatie via besloten netwerken, bijvoorbeeld van bedrijven of overheidsinstellingen (artikel 13.7). De Kamer heeft dit artikel ondanks scherpe kritiek hierop van onder meer de Registratiekamer en het VNO/NCW aanvaard. In de Nota WES wordt op deze kwestie niet voldoende ingegaan. In de praktijk raken besloten en openbare netwerken steeds meer onderling verweven. Voor de gebruiker dient voorzienbaar te zijn welke inbreuken op zijn persoonlijke levenssfeer en op zijn communicatievrijheid in het bijzonder mogelijk zijn. Het is zaak deze kwestie meer systematisch te doordenken. De gang van zaken rond de behandeling van artikel 13.7 Telecomwet dient in de toekomst te worden vermeden.

Als het gaat om het toepassen van bijzondere opsporingsbevoegdheden op de elektronische snelweg ondersteunt de Registratiekamer de zienswijze van het kabinet dat in de wetgeving nauwkeuriger onderscheid moet worden gemaakt tussen het verkrijgen van reeds opgeslagen gegevens en het vergaren van gegevens die in de toekomst beschikbaar komen. Niet lichtvaardig mag tot een verplichting worden overgegaan aan netwerkaanbieders om gegevens ten behoeve van de opsporing te verzamelen (blz. 81-82). Helaas constateert de Registratiekamer dat in artikel 13.4 van de door uw Kamer aanvaarde Telecommunicatiewet een gevaarlijk precedent is geschapen doordat een vergaande vergaringsverplichting is opgelegd aan telecomaanbieders om, anders dan voor de eigen bedrijfsvoering, persoonsgegevens vast te leggen van personen ten aanzien van wie nog geen - begin van- verdenking bestaat. De hiervoor geschetste technische mogelijkheden van datamining versterken de risico’s van een onaanvaardbare inbreuk op de bescherming van niet verdachte burgers aanzienlijk.

In het algemeen is de Registratiekamer daarbij van oordeel dat de rechtsbescherming van gebruikers van elektronische communicatie beter zou zijn gediend met een stelsel van waarborgen dat zich op het gehele proces van verwerking van informatie richt, ongeacht de fase waarin de communicatie zich bevindt of de plaats waar. Een dergelijke

benadering doet recht aan de huidige stand van ICT. De Registratiekamer wijst er hierbij op dat in de (aanstaande) Wet bescherming persoonsgegevens ook gekozen is voor een procesmatige benadering: in plaats van het aanleggen van een persoons*registratie* (onder de Wet persoonsregistraties) wordt het centrale begrip *verwerking* van persoonsgegevens.

5. Encryptie

In het kader van het verzekeren van de betrouwbaarheid en afscherming van de communicatie op de elektronische snelweg speelt encryptie een onmisbare rol. Dit wordt ook door het kabinet onderkend. In de Nota WES neemt het kabinet het standpunt in dat verbod van cryptografieprodukten niet aan de orde is en dat de eisen die de overheid stelt op dit terrein, niet verder zullen gaan dan het in het leven roepen van een medewerkingsverplichting van aanbieders van diensten bij het in voorkomende gevallen ontsleutelen van berichten. Met betrekking tot (zware vormen van) cryptografie ziet het kabinet uitdrukkelijk een rol weggelegd voor de Trusted Third Parties (TTP's). De Registratiekamer heeft in haar jaarverslag (blz. 102) gesteld, dat er meerdere TTP's met een concurrerend belang dienen te worden opgericht met een scheiding tussen TTP diensten voor authenticiteit en integriteit en TTP diensten voor vertrouwelijkheid. De Registratiekamer dringt er tevens op aan (blz. 103) dat er op korte termijn een onafhankelijke toezichthoudende en actief stimulerende TTP-kamer moet komen, die minimum eisen en randvoorwaarden stelt aan TTP's. Keuzevrijheid in TTP's acht zij van groot belang.

Hiermee in flagrante tegenspraak is de aankondiging van de Minister van Binnenlandse zaken van 18 februari j.l. in een brief aan uw Kamer (Kamerstukken II, 1997-1998, 21 501-10, nr. 38) van een deponeringsplicht van cryptografische sleutels bij de overheid. In haar reactie van 9 april jl. heeft de Registratiekamer gewezen op deze discrepantie in het standpunt van het kabinet en de Minister van Binnenlandse zaken. Zij heeft voorts het belang benadrukt van encryptie en van TTP voor het vertrouwen dat de burger kan stellen in de digitale snelwegen. Betrouwbare encryptie acht zij onmisbaar voor het behoud van privacy en voor de ontwikkeling van electronic commerce. Deze reactie heeft zij ook aan uw Kamer doen toekomen.

6. Conclusie

De Registratiekamer heeft slechts enkele elementen belicht uit de Nota WES, waarin veel aan de orde wordt gesteld en waarbij het zicht op de beleidsvoornemens soms gehinderd wordt door de gelaagdheid van de behandeling van onderwerpen. Indien door het kabinet aangekondigde voorstellen daartoe aanleiding geven zal zij hierop nader reageren.

Op de gehele materie die in de Nota WES aan de orde wordt gesteld is van toepassing hetgeen de Registratiekamer in haar jaarverslag over 1997 opmerkte:
“De faciliterende functie van technologie komt pregnant tot uiting op het terrein van de telecommunicatie. De grenzen tussen vaste telefoon, mobiele telefoon, internet en televisiekabel vervagen. De overheid probeert op nieuwe vormen van informatietechnologie maximale greep te verwerven. Hierbij komt niet alleen de vrijheid van meningsuiting op bijvoorbeeld internet in de knel. Ook de privacybescherming komt onder druk te staan ten gevolge van deze ontwikkelingen. Nieuwe vormen van digitaal dataverkeer maken het traceren van gebruikers (het dataverkeer) en het analyseren van het gebruik (de boodschap) gemakkelijker. Politie, justitie en inlichtingen- en veiligheidsdiensten verstevigen hun greep. Het uitgangspunt dat de *off line* geldende (grond)rechten *on line* evenzeer behoren te worden gerespecteerd dient kennelijk te worden bevochten. De paradox van de modernisering en de ontwikkeling van nieuwe vormen van telecommunicatie is dat die samengaat met minder waarborgen voor vertrouwelijkheid en minder mogelijkheden om met behoud van privacy van telecommunicatiefaciliteiten gebruik te maken. Dit kan aan de acceptatie van met name electronische dienstverlening in de weg staan. De overheid dient zich garant te stellen voor het behoud van grondrechten waaronder met name de bescherming van de persoonlijke levenssfeer en het communicatiegeheim bij het gebruik van nieuwe vormen van telecommunicatie. Ook de liberalisering van de markt is een factor van betekenis. Meer aanbieders van telecommunicatiefaciliteiten leidt tot meer bestanden van persoonsgegevens en maakt controle en toezicht op het gebruik van die bestanden moeilijker. De ontwikkeling van de informatie-infrastructuur en de ontwikkelingen op bovengenoemde terreinen zullen ongetwijfeld aan de orde komen bij

het regeerakkoord. De Registratiekamer dringt er op aan dat het waarborgen van de privacybescherming daarbij niet het sluitstuk wordt. De ontwikkeling van nieuwe informatie-infrastructuren en van nieuwe informatierelaties in en tussen de publieke en private sector heeft aanzienlijke gevolgen voor de verwerking, het gebruik en de bescherming van persoonsgegevens. Die gevolgen moeten in een vroeg stadium worden onderkend en een permanent onderdeel zijn in het beslissingsproces." (blz. 11-12)

De mogelijkheid voor het geven van een toelichting op het voorgaande zal aanwezig zijn tijdens de door u te houden hoorzitting op 3 september.