

Vergaderjaar 1998–1999

25 880

Wetgeving voor de elektronische snelweg

Nr. 3

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 31 december 1998

De vaste commissie voor Justitie¹ heeft over de Nota «wetgeving voor de elektronische snelweg» (25 880, nr. 2) een aantal vragen ter beantwoording aan de regering voorgelegd. Deze vragen, alsmede de daarop gegeven antwoorden zijn hieronder afgedrukt.

De voorzitter van de commissie,
Van Heemst

De griffier voor deze lijst,
Del Grosso

¹ Samenstelling:

Leden: Van de Camp (CDA), Biesheuvel (CDA), Swildens-Rozendaal (PvdA), Scheltema-de Nie (D66), Kalsbeek-Jasperse (PvdA), Zijlstra (PvdA), Apostolou (PvdA), Middel (PvdA), Van Heemst (PvdA), voorzitter, Dittrich (D66), ondervoorzitter, Rabbae (GL), Rouvoet (RPF), Van Oven (PvdA), O. P. G. Vos (VVD), Van Wijmen (CDA), Patijn (VVD), De Wit (SP), Ross-van Dorp (CDA), Niederer (VVD), Nicolai (VVD), Halsema (GL), Weekers (VVD), Van der Staaij (SGP), Wijn (CDA) en Brood (VVD).

Plv. leden: Balkenende (CDA), Verhagen (CDA), Wagenaar (PvdA), Van Vliet (D66), Arib (PvdA), Duijkers (PvdA), Kuijper (PvdA), Albayrak (PvdA), Barth (PvdA), De Graaf (D66), Karimi (GL), Schutte (GPV), Santi (PvdA), Van den Doel (VVD), Rietkerk (CDA), Rijpstra (VVD), Marijnissen (SP), Buijs (CDA), Passtoors (VVD), Van Blerck-Woerdman (VVD), Oedayraj Singh Varma (GL), De Vries (VVD), Van Walsem (D66), Van der Hoeven (CDA) en Kamp (VVD).

VRAGEN

1

In hoeverre is onderzocht of de technologie oplossingen kan bieden voor de juridische problemen waar de elektronische snelweg de overheid en de samenleving voor stelt?

2

Geldt de bescherming van jeugdigen tegen schadelijke invloeden ook voor volwassenen bestemde advertentie-uitingen op Internet? Zo ja, op welke wijze kan een dergelijk voornemen gestalte krijgen?

3

Wordt de elektronische snelweg ten principale beschouwd als openbare ruimte of als private onderneming?

4

Uitgangspunt is dat wat «off line» geldt, ook «on line» moet gelden. Het is evenwel denkbaar dat het elektronisch domein maatschappelijke vernieuwing genereert. In dat geval kan wat «on line» geldt, «off line» gaan gelden. Maar ook dan moeten de rechtsregels in beide gebieden gelijk zijn. Kan hiervan een of meerdere voorbeelden worden gegeven? (blz. 5).

5

Kunnen er voorbeelden worden gegeven van gevallen waarin sprake is van verdringing? (blz. 5).

6

Kan nader worden ingegaan op de modelwet van UNCITRAL? Is dit het enige model waarnaar gekeken is? Waarom is voor deze modelwet gekozen? (blz. 6).

7

Wat is de stand van zaken met betrekking tot het opstellen van specifiek internationaal privaatrecht op dit moment? (blz. 6).

8

Waarom wordt een specifieke privaatrechtelijke aansprakelijkheidsregeling voor tussenpersonen niet overwogen? (blz. 6).

9

De elektronische handel maakt het buitenlandse aanbieders eenvoudig vergunningenvereisten te omzeilen. Een voorstel is om deze aanbieders te verplichten in de EU een vertegenwoordiger aan te wijzen. Over de implicaties van dit voorstel vindt nader onderzoek plaats. Wat is de stand van zaken? (blz. 6).

10

Kan nader worden ingegaan op de problematiek van encryptie en wat de overheid daartegen meent te gaan doen? (blz. 6).

11

Zou het voornemen om in de AWB een experimenteerbepaling op te nemen waarbij elektronische documenten onder voorwaarden gelijk worden gesteld met schriftelijke documenten kunnen worden uitgebreid tot de Wet Openbaarheid van Bestuur? (blz. 6 en 73).

12

Op welke wijze vindt controle plaats op zelfregulering? (blz. 7).

13

Onderschrijft de regering, ook na recente ontwikkelingen op dit gebied, dat op de bestrijding van kinderporno nog steeds een belangrijke rol valt toe te kennen aan zelfregulering? (blz. 7 en 80).

14

Er moeten regels komen voor de omvang van de rechtsmacht, waarbij een prioriteit wordt afgesproken over de uitoefening van de rechtsmacht. De «aanknopingspuntenleer» uit het bestaande internationaal privaatrecht kan hierbij een rol spelen. Kan dit nader worden toegelicht? (blz. 8).

15

Wat wordt verstaan onder handhavingsautoriteiten? Werken zij al samen? (blz. 8).

16

Wat is de stand van zaken omtrent de zogenoemde pragmatische meersporenaanpak inzake internationalisering en rechtsmacht? (blz. 8).

17

Is een begin gemaakt met de internationale harmonisatie van materiële normen? En hoe krijgt deze harmonisatie gestalte? (blz. 8).

18

Wat houdt de «vereiste van dubbele strafbaarheid» precies in? (blz. 8).

19

Wordt gedacht aan het opstellen van een gedragscode voor de privaatrechtelijke en strafrechtelijke aansprakelijkheid van tussenpersonen? (blz. 8).

20

Op welke termijn wordt gedacht de elektronische toegang tot openbare registers te verwezenlijken? Zullen openbare overheidsarchieven ook bij dit voornemen worden betrokken? (blz. 9).

21

Kan een voorbeeld/kunnen voorbeelden worden gegeven van verdringing, dus die gevallen waarin de burger niet vrij is in zijn keuze om van de elektronische snelweg gebruik te maken? (blz. 9).

22

De overheid kan een rol spelen bij de toewijzing van adressen en domeinnamen. Op welke wijze, naast ondersteuning van de Stichting Internet Domeinregistratie, denkt de overheid dit te doen? (blz. 10).

23

Datamining vormt een tot nu toe onderschatte inbreukmogelijkheid op de privacy. Wat is het standpunt van de regering op het punt van datamining? Wat is de stand van zaken omtrent het onderzoek naar datamining als opsporingstechniek? Welke beperkingen moeten er aan datamining gesteld worden? (blz. 7, 11 en 88).

24

In welke fase bevindt zich de besluitvorming in de Raad van Europa inmiddels? Welke rol speelt Nederland daarbij? (blz. 11 en 116).

25

Wat is de stand van zaken betreffende afspraken die binnen het kader van de Raad van Europa moeten worden gemaakt over specifieke rechtsmachtvraagstukken? (blz. 11).

26

Hoe ver is het met de regelgeving over de digitale handtekening? (blz. 11).

27

Aan welke voorbeelden wordt gedacht bij het versterken van de concurrentiepositie van Nederland? Hoe verhoudt nationale wetgeving zich dit voornemen (en deze voorbeelden) tot Europese (mededingings-) wetgeving? (blz. 13).

28

De overheid draagt zorg voor de naleving van de voorwaarden waaraan zelfregulering moet voldoen. Zo zou zij onvoldoende vertegenwoordigde belangen kunnen behartigen. Kan hiervan een voorbeeld worden gegeven? (blz. 13).

29

Wat is de stand van zaken ten aanzien van de aangekondigde nota's en aktieplannen? (blz. 24).

30

Waarop is de mening van de regering gebaseerd dat E-mail wordt gezien als een informeel communicatiemiddel? Hoe denkt de regering te bereiken dat de positie van de klassieke media onaangestast blijft? Hoe krijgen nieuwe ontwikkelingen een plaats in het regeringsbeleid? (blz. 29).

31

Waarom is het belangrijk dat de positie van de klassieke media onaangestast blijft? (blz. 29).

32

Hoe kan worden bevorderd dat Internet en andere elektronische diensten van luxegoed tot gemeengoed worden? Welke categorieën maken er nu voornamelijk gebruik van? (blz. 29).

33

Volgens de Nota is er moeilijk een onderscheid te maken tussen transport en opslag. Hoe zit het in dit kader met de juridische term «bezit»? Heeft een ieder die een Internetaansluiting heeft ook (passief) illegale uitingen op het net in bezit? (blz. 50).

34

Hoe verhoudt/verhouden (voornemens tot) nationale ordening zich tot het internationale karakter van de Elektronische Snelweg? Op welke politieke en juridische problemen stuit dit? (blz. 58).

35

In de nota wordt gekozen voor de dominantie van de ordenende overheid. Waarop baseert de regering de mening dat de rol van de overheid tot ordening moet worden beperkt? (blz. 58).

36

Wanneer gaat de regering een besluit nemen omtrent Trusted Third Parties? Welke rol ziet de overheid weggelegd voor Trusted Third Parties in het kader van privacy en eigendomsbescherming? (blz. 64).

37

In hoeverre blijft de huidige omschrijving van een toerekenbare onrechtmatige daad gelijk voor handelingen op de elektronische snelweg? In hoeverre is het gevaar aanwezig dat juist door de technologie de huidige omschrijving niet meer handhaafbaar blijkt te zijn? (blz. 66).

38

Internationaal privaatrecht is een van de noodzakelijke zaken die bekeken moeten worden op hun toepasbaarheid voor Internet en de elektronische snelweg. Eigenlijk is Internet «footloose» als het gaat om rechtsverhoudingen. Welke pogingen zijn er inmiddels in het werk gesteld om dit probleem in kaart te brengen en aan te pakken? (blz. 68–70).

39

Waarop is de stelling gebaseerd dat de algemene begrippen van het vermogensrecht in het Burgerlijk Wetboek technologie-onafhankelijk zijn? In hoeverre zijn deze algemene begrippen handhaafbaar op de elektronische snelweg? (blz. 70).

40

Hoe verhouden de voornemens met betrekking tot de AWB zich tot de uit recente evaluatie van de AWB gebleken gebrek aan tijdigheid bij veel lagere overheden? Is de deskundigheid voor elektronisch verkeer bij alle overheidslagen wel voldoende aanwezig? (blz. 73).

41

De regering stelt voor om de AWB aan te vullen met een experimenteerbepaling waarbij bestuursorganen onder nader te bepalen voorwaarden de bevoegdheid krijgen om elektronische documenten gelijk te stellen met schriftelijke documenten, alsmede om in verband daarmee zo nodig nadere voorschriften te stellen. Waarom een experimenteerbepaling? Waarom geen algemeen geldende richtlijnen of voorschriften? (blz. 75).

42

Welke reikwijdte ziet de regering aan het begrip «zelfregulering» bij de aansprakelijkheid van providers? Welke criteria gaat de regering hanteren ten aanzien van zelfregulering en het beoordelen van de kwaliteit van zelfregulering? Op welke wijze denkt de regering invulling te gaan geven aan het toezicht op de kwaliteit van zelfregulering? Welke juridische status gaat zelfregulering krijgen? (blz. 85).

43

De vraag ten aanzien van de technologie-onafhankelijke formulering geldt ook het strafrecht. Hoe wordt hiermee rekening gehouden? Het gaat niet alleen om een technologie onafhankelijke formulering, het gaat ook om opspoorbaarheid en handhaafbaarheid. (blz. 85).

44

In hoeverre is de regering voornemens om met behulp van nieuwe technologie juridische en strafrechtelijke problemen aan te pakken? (blz. 85).

45

Is een aanpassing van artikel 350a van het Wetboek van Strafrecht gewenst? (blz. 85).

46

Wat is de stand van zaken met betrekking tot de nieuwe Europese richtlijn over auteursrecht en naburige rechten? (blz. 87).

47

In hoeverre is de regering voornemens om de digitale recherche (meer) vorm en inhoud te geven? Op welke wijze gaat worden voorzien in training en opleiding op dit punt? Is er eigenlijk niet al gedurende langere tijd sprake van een behoorlijke achterstand binnen het opsporingsap-

paraat ten aanzien van kennis en vaardigheden op het terrein van digitale recherche?

48

Welke visie heeft de regering op het begrip universele dienstverlening in relatie tot de elektronische snelweg? (blz. 95).

49

«Alle telecommunicatienetwerken moeten zijn af te tappen.» Waarop is deze mening c.q. vooronderstelling gebaseerd? Houdt de aftap-technologie wel gelijke tred met de telecommunicatietechnologie? Wie is eigenlijk aanspreekbaar (ook financieel) voor het aftapbaar zijn van telecommunicatienetwerken? (blz. 95).

50

Heeft het onderzoek over de aanpassing van artikel 7 van de Grondwet inmiddels tot concrete(re) voorstellen geleid? (blz. 100).

51

Loopt de voorgenomen aanpassing van artikel 7 van de Grondwet in gelijke pas met de technologische ontwikkelingen? Zo ja, waarop is deze vooronderstelling gebaseerd? (blz. 100).

52

Wel niveau van supranationale regelgeving is het meest gewenst? Welke initiatieven binnen welke kaders heeft Nederland ondernomen om tot supranationale regelgeving te komen? (blz. 118).

53

Zijn er voorbeelden van internationale zelfregulering? Spelen Nederlandse providers daarbij een rol? (blz. 120).

54

Is het algemene uitgangspunt: wat off-line geldt, geldt ook on-line niet lastig uitvoerbaar gelet op het wereldwijde karakter van Internet? Hoe wordt bijvoorbeeld omgegaan met de toepasbaarheid van het Nederlands recht bij electronic commerce? (blz. 121).

55

Wat is de stand van zaken met betrekking tot het opstellen van internationaal privaatrecht ten aanzien van Internet? (blz. 121).

56

Zijn de voorgestelde maatregelen van de overheid op het gebied van de bescherming van persoonsgegevens wel toereikend, wanneer deze toch voornamelijk liggen op het terrein van voorlichting en het stimuleren van harmonisatie van internationale normen en het stimuleren van zelfregulering? Zijn er op de elektronische snelweg minder waarborgen voor de bescherming van persoonsgegevens? Stelt de overheid zich desondanks volgens de voorstellen in de nota terughoudender op dan off-line het geval is? Kunnen burgers zich dan in beginsel wel anoniem op de digitale snelweg begeven? (blz. 123–133, 170 en 200).

57

Wat is de stand van zaken op het gebied van de ontwikkeling persoonsverificatie met behulp van biometrie? Standaardisatie kan volgens de regering via zelfregulering plaatsvinden. Is dit wel reëel, gelet op de eisen die standaardisatie kan stellen op het gebied van de privacy? Van de andere kant acht de regering een nadere wettelijke regeling gewenst. Op welke gebieden is die nadere regeling gewenst? Wordt internationale

regelgeving op dit terrein afgewacht of is de regering voornemens om nu reeds een aanvang te maken met de benodigde nationale regelgeving? (blz. 128).

58

Bij een van de middelen om de privacy te waarborgen, de private enchancing technologies (PET), wordt overwogen om mogelijkheden open te laten om persoonsgegevens te kunnen achterhalen. De andere optie zou zijn om een algehele identificatie- en registratieplicht bij het betreden van de elektronische snelweg in te stellen. Hoe verhouden deze opties zich het uitgangspunt dat wat off-line geldt ook on-line moet gelden? In de off-line situaties is er toch ook geen sprake van een situatie waarbij de identiteit altijd bij een van de actoren bekend is, evenmin als een situatie waarin sprake is van een algehele identificatie- en registratieplicht. (blz. 130 en 162).

59

Zou één centraal aanspreekpunt niet duidelijker zijn voor burgers dan het benoemen van zoveel mogelijk privacyfunctionarissen? (blz. 132).

60

Op welke wijze denkt de regering de handhaafbaarheid van de strafrechtelijke bescherming van e-mail te gaan regelen? (blz. 133).

61

Welke lering is er omtrent de aanpak van het millenniumvraagstuk te trekken ten aanzien van de betrouwbaarheid van de nieuwe techniek en het elektronisch berichtenverkeer? (blz. 134).

62

Zijn er gebieden aan te wijzen waarop het functioneren van de overheid reeds te afhankelijk is geworden van digitale technieken? (blz. 134).

63

Het ligt in het voornemen om ten aanzien van Trusted Third Parties een aantal eisen te stellen. In die eisen kan worden voorzien via zelfregulering, onderbouwd door een stelsel van overheidstoezicht. Deze constructie doet enigszins gekunsteld aan. Hoe denkt de regering de afzonderlijke verantwoordelijkheden dan te regelen? (blz. 145).

20a

Welke mogelijkheden zijn er om toegankelijkheid en pluriformiteit van media te blijven garanderen? Speelt het «eigenaarschap» van het Internet daarbij een rol (vgl. kabelexploïtatie)? (blz. 153).

64

Mag er een monopolie bestaan op overheidsinformatie? Bieden nieuwe technologieën extra mogelijkheden om overheidsinformatie een meer openbaar en toegankelijk karakter te geven? Zo ja, op welke wijze zullen deze de komende jaren worden benut? (blz. 157).

65

Gegevens in digitale elektronische informatie- en communicatienetwerken kunnen in snel wisselende toestanden van transport of opslag verkeren of zelfs in beide toestanden tegelijk verkeren. Het onderscheidend criterium van de regering is: valt een gegeven te raadplegen op een door de mens te bepalen tijdstip?

Kan dit onderscheid door de wetgever gehanteerd blijven, gezien het feit dat transport bestaat uit opslag en transmissie? Is het niet mogelijk om gegevens die bij het transport tijdelijk worden opgeslagen te raadplegen?

Vervalt hiermee niet het onderscheid tussen opslag en transport? (blz. 159–160).

66

Kunnen de onder 4.2. genoemde vier uitgangspunten met betrekking tot strafrechtelijke handhaving niet met elkaar in strijd komen? Zo ja, welk(e) uitgangspunt(en) zal dan prioriteit krijgen bij de handhaving van het strafrecht? (blz. 168).

67

Wanneer internet service providers verplicht zouden worden om, ten behoeve van de opsporing van strafbare feiten, bij te houden welke handelingen abonnees verrichten, zou dit een eerste stap kunnen zijn op weg naar vergaande inbreuk op de bescherming van privacy van alle gebruikers van de snelweg. Ziet de regering dit desondanks toch als een bruikbare mogelijkheid om strafbare feiten op te sporen? Treft deze vorm van datamining niet ook burgers ten aanzien van wie nog niet enige verdenking bestaat van betrokkenheid bij een strafbaar feit of het in gevaar brengen van de staat? Is de regering van mening dat de Wet bescherming persoonsgegevens op dit punt voldoende bescherming zal bieden? (blz. 169).

68

In de nota staat vermeld dat voor de zomer van 1998 de Tweede Kamer nader zal worden geïnformeerd over de voornemens op het gebied van opleiding, organisatie en uitrusting van politie- en justitiefunctionarissen met het oog op de elektronische snelweg. Hoever staat het daarmee? Welke voornemens zijn er? Welk budget? (blz. 169).

69

Bij de 5 centrale thema's speelt zelfregulering een zeer belangrijke rol. De overheid heeft slechts een ordenende functie. De gebruikers en aanbieders op de elektronische snelweg worden allereerst zelf verantwoordelijk geacht. Is er dan nog wel sprake van: «Wat off-line geldt moet ook on-line gelden»? (blz. 170).

70

Kan de regering precies aangeven op welke terreinen zij zelfregulering een goed c.q. noodzakelijk instrument acht en op welke terreinen niet? Welke afwegingskader wordt daarbij gehanteerd? (blz. 185 e.v.).

71

Aan de Interdepartementale Commissie voor de Harmonisatie van Wetgeving wordt verzocht het toetsingskader mee te nemen bij de eerstvolgende wijziging van de Aanwijzing voor de regelgeving en hierover advies uit te brengen. Op welke termijn kan dit tegemoet worden gezien? (blz. 192).

72

In de nota staan ongelooflijk veel beleidsvoornemens. Kan de regering aangeven welk tijdpad men eigenlijk voor ogen heeft bij het realiseren van al deze plannen? Kan ook worden aangegeven welke wetsvoorstellen in deze regeerperiode kunnen worden verwacht? In hoeverre is het actieplan vanaf blz. 195 eigenlijk nog van toepassing? (blz. 194 e.v.).

73

Hoe verhoudt dit Actieplan zich tot de voornemens uit het regeerakkoord? Zijn er inmiddels aanpassingen op genoemde schema's? (blz. 194).

ANTWOORDEN

Inleiding

De nota Wetgeving voor de elektronische snelweg heeft bij uw Kamer veel belangstelling gewekt. Dit blijkt niet alleen uit de vragen die aan de regering zijn voorgelegd, maar bijvoorbeeld ook uit de hoorzitting van 3 september jl. over deze nota en uit het debat met mijn voorgangster tijdens het algemeen overleg over de notitie Boven NAP.

Ik verheug mij over die belangstelling. De vaak fundamentele vraagstukken, die de nota aan de orde stelt, behoren naar mijn oordeel voorwerp te vormen van een maatschappelijk debat, waarbij het gaat over de toekomstige positie van de wetgever – en daarmee van de overheid – in een informatiesamenleving.

Alvorens op de afzonderlijke vragen in te gaan, lijkt het mij nuttig enige algemene opmerkingen te maken over de nota, die onder de verantwoordelijkheid van mijn voorgangster tot stand is gekomen. Ik richt mij daarbij op drie hoofdpunten:

- de *aard* van de overheidsinterventie: «wat «off line» geldt, moet ook «on line» gelden».
- de *omvang* van de overheidsverantwoordelijkheid in relatie tot de verantwoordelijkheid van de particuliere sector, of bezien vanuit de behoefte van regulering: waar is wetgeving nodig en waar is zelfregulering het meest geëigende instrument?
- de gevolgen van de internationalisering: waar liggen de beperkingen voor nationale ordening en waar kan zo'n nationale ordening juist bij uitstek een nuttige rol vervullen?

Het zijn deze drie hoofdpunten die ook bij veel van de door uw Commissie aan mij gestelde vragen een rol spelen.

De aard van de overheidsverantwoordelijkheid

De nota draagt over de aard van de overheidsverantwoordelijkheid de volgende filosofie uit:

- In deze fase van ontwikkeling van de elektronische snelweg zijn bestaande kaders en rechtsnormen geschikt voor toepassing in de elektronische omgeving; soms zijn echter aanpassingen nodig.
- De overheid dient er voor te zorgen dat deze kaders en rechtsnormen, die voor de fysieke wereld zijn ontwikkeld, ook daadwerkelijk in de elektronische omgeving kunnen worden toegepast. Wat «off line» geldt, moet ook «on line» gelden.
- Bij de invulling van deze taak houdt de overheid rekening met drie specifieke kenmerken van de elektronische snelweg, te weten dematerialisering, internationalisering en technologische turbulentie.

Het is mij gebleken dat met name veel discussie ontstaat over het uitgangspunt «wat «off line» geldt, moet ook «on line» gelden.»

Ik zie dit uitgangspunt als volgt. Op de elektronische snelweg dienen dezelfde rechtsnormen en waarden te gelden als in de fysieke wereld. Om die toestand te bereiken zullen in beginsel «on line» en «off line» dezelfde rechtsinstrumenten (rechtsregels) worden ingezet. Soms zal aanvullend de inzet van andere – specifiek op de elektronische snelweg toegesneden – rechtsinstrumenten nodig zijn.

Ik ben van mening dat wij het uitgangspunt overeind moeten houden. Zeker naar mate elektronische communicatie en elektronisch zakendoen zich ontwikkelen tot voor veel burgers normale handelingen, is er geen reden voor deze handelingen een afwijkend normenkader te ontwikkelen. Burgers moeten er van uit kunnen gaan dat hetzelfde recht hen beschermt, onafhankelijk van de vraag of zij zich op een zeker moment op de elektronische snelweg bevinden of juist niet.

De inspanning van de overheid zal er op gericht moeten zijn dat de normen die voor de fysieke wereld zijn ontwikkeld ook daadwerkelijk toepasbaar zijn in de elektronische omgeving en ook kunnen worden gehandhaafd.

Invulling van deze inspanning kan per geval verschillen:

- Soms zullen normen eenvoudigweg toepasbaar moeten worden gemaakt: waar de wetgever het vereiste van schriftelijke communicatie stelt, zal ruimte worden geschapen voor een elektronisch alternatief.
- In andere gevallen zal de norm zelf nadere invulling behoeven. Ik noem als voorbeeld de zorg voor een betrouwbaar rechtsverkeer. In een elektronische omgeving, waar partijen elkaars identiteit vaak niet eens zullen kennen, is een grotere behoefte aan bescherming van de betrouwbaarheid van het rechtsverkeer. De overheid kan die extra bescherming bieden door het opstellen van wettelijke bepalingen, maar ook – of in aanvulling daarop – door de totstandkoming van zelfregulering te bevorderen en daarop toe te zien.
- Ook vergt de handhaving van normen in de elektronische omgeving soms extra voorzieningen. De mogelijkheid in een elektronische omgeving identiteit en plaats van handelen te verhullen is hieraan vaak debet.

Het is niet te voorzien in hoeverre het adagium «wat «off line» geldt, moet ook «on line» gelden» ook op langere termijn in alle gevallen toepasbaar blijft. Dit hangt af van de ontwikkeling en het gebruik van de elektronische communicatie. De nota noemt in dit verband de fase waarin de elektronische snelweg traditionele communicatiemiddelen verdringt. Dan zou het onjuist zijn steeds uit te gaan van voor de traditionele omgeving ontwikkelde normen.

Daarnaast kan het zo zijn dat zich in een verdere toekomst daadwerkelijk nieuwe rechtsbeginselen ontwikkelen, omdat bestaande concepten niet meer volstaan. Ik sluit bijvoorbeeld niet uit dat het recht op privacy een heel nieuwe impact krijgt indien een groot deel van de menselijke communicatie via elektronische middelen plaatsvindt.

Op dit moment bevindt het denken over nieuwe rechtsbeginselen zich nog in een zeer pril stadium. Het kabinet zal de nationale en internationale discussies daaromtrent actief volgen en, waar nodig, stimuleren. Daarbij ga ik er wel vanuit dat nieuwe rechtsnormen zich in de samenleving dienen te ontwikkelen. Een en ander betekent niet dat op dit moment aan de toepasbaarheid van het adagium moet worden getwijfeld.

De omvang van de overheidsverantwoordelijkheid

Het tweede hoofdpunt, waar ik op inga, ziet op de omvang van de overheidsverantwoordelijkheid en de verantwoordelijkheid van de private sector. De nota schetst drie taken voor de overheid. Ter herinnering, dit zijn:

- het waarborgen van een aantal fundamentele normen en waarden van de democratische rechtsstaat in de elektronische omgeving.
- het faciliteren van het elektronisch maatschappelijk verkeer.
- het garanderen van de elementaire voorzieningen die nodig zijn voor het maatschappelijk functioneren van burgers en bedrijven in een informatiesamenleving.

De specifieke kenmerken van de elektronische snelweg – demateriali-

sering, internationalisering en technologische turbulentie; ik noemde ze reeds eerder – bepalen de invulling van die taken. Alternatieven voor formele wetgeving verdienen vaak de voorkeur; een zelfde voorkeur geldt technologie-onafhankelijke formuleringen in regelgeving. Flexibiliteit staat derhalve voorop; dit mag echter niet ten koste gaan van de rechtszekerheid, zeker waar fundamentele waarden van de democratische rechtsstaat in het geding zijn.

In concrete gevallen moet het toetsingskader uit Deel D van de nota een houvast geven bij de afweging over de vraag of zelfregulering een geschikt instrument is als alternatief voor wetgeving.

Een en ander betekent voor de drie taken het volgende.

De eerste taak betreft het waarborgen van fundamentele waarden en normen. Duidelijk is dat de wetgever deze taak niet kan overlaten aan de private sector. Het gaat hier immers om de kern van de rechtsstaat. Wel kan zelfregulering een aanvullende rol spelen. Het Internet Meldpunt kinderporno is opgezet om uitdrukking te geven aan de maatschappelijke verantwoordelijkheid van de Internetproviders. Op deze wijze kan een stelsel van zelfregulering ondersteunend werken aan de opsporing van deze ernstige strafbare feiten door de overheid zelf.

Ter uitvoering van de tweede taak draagt de overheid zorg voor een juridische infrastructuur, die een adequaat en veilig rechtsverkeer mogelijk maakt. Juist bij de uitvoering van deze taak verdient zelfregulering – ter invulling van algemene (privaatrechtelijke) wettelijke uitgangspunten – de voorkeur. Marktpartijen zelf zijn vaak het best in staat op flexibele wijze regels te stellen voor de specifieke situaties waarvoor de elektronische snelweg hen stelt. Zelfregulering is in veel, doch zeker niet alle gevallen, een geschikt instrument om publieke belangen te waarborgen.

Deze zelfregulering moet wel aan een aantal randvoorwaarden voldoen. Immers, het gaat hier om zelfregulering die invulling geeft aan de publieke taak het elektronisch rechtsverkeer te faciliteren. In het toetsingskader uit de nota zijn die randvoorwaarden geëxpliciteerd; tevens is aangegeven op welke wijze de overheid toeziet op naleving van die voorwaarden. Als voorbeeld wijs ik op het totstandbrengen van een gedragscode voor elektronisch zakendoen, ter uitvoering van het Actieplan Electronic Commerce van april 1998. Deze gedragscode wordt opgesteld door private partijen in nauw overleg met de ministeries van Economische Zaken en Justitie. Tegelijkertijd wordt een wijziging van het Burgerlijk Wetboek voorbereid; deze wijziging kan de gedragscode ondersteunen.

Het toezicht door de overheid kan op verschillende manieren vorm krijgen. Als uiterste middel heeft de overheid natuurlijk altijd de mogelijkheid tot wetgeving over te gaan, indien geen zelfregulering tot stand komt, of indien de zelfregulering niet aan de gestelde eisen voldoet. In het laatste geval zal dit kunnen leiden tot onverbindendheid van via zelfregulering tot stand gekomen normen.

De derde taak, zo stelt de nota, leidt op dit moment niet tot de inzet van juridisch instrumentarium. Zolang het gebruik maken van elektronische voorzieningen geen voorwaarde vormt voor normaal maatschappelijk functioneren, is het geen taak van de overheid de toegang daartoe te garanderen. Het kabinet volgt daarmee de internationale communis opinio dat het tot stand brengen van elektronische voorzieningen in de eerste plaats een zaak is van marktpartijen. De overheid ziet daar wel op toe, onder meer via het mededingingsinstrumentarium. Ook het instrument van universele dienstverlening uit hoofdstuk 9 van de

Telecommunicatiewet kan zo nodig van toepassing worden op nieuwe communicatiemiddelen.

Internationalisering

De internationalisering, het derde hoofdpunt waar ik op inga, brengt de grenzen van de overheidsbevoegdheid in zicht. De nota omschrijft dit terecht als het meest fundamentele vraagstuk waarvoor de elektronische snelweg ons stelt. Via een combinatie van maatregelen – de pragmatische meersporenaanpak, zo noemt de nota het – tracht de nota een aanzet te geven voor een oplossing. Zo'n oplossing zal in grote lijnen in internationaal verband tot stand moeten komen.

Internationaal gaan de ontwikkelingen op dit moment snel. Ik noem:

- de OESO heeft in oktober in Ottawa een ministeriële conferentie georganiseerd, waarin tezamen met het bedrijfsleven is gewerkt aan internationale afspraken over elektronisch zakendoen. Deze conferentie heeft geleid tot verklaringen over privacy, authenticatie, consumentenbescherming en belastingen;
- de vele activiteiten van de Europese Commissie op dit terrein hebben op 18 november 1998 een voorstel voor een richtlijn over juridische aspecten van elektronisch zakendoen opgeleverd;
- in de Raad van Europa wordt goede voortgang geboekt met het verdrag over «crime in Cyber-space».
- Binnen UNCITRAL – de VN-organisatie voor internationaal handelsrecht – wordt gewerkt aan een modelwet inzake elektronische handtekeningen en certification authorities, waarbij wordt voortgebouwd op de modelwet inzake elektronisch zakendoen van 1996.

De Nederlandse regering richt zijn inbreng zoveel mogelijk op deze lopende ontwikkelingen. Daarbij blijkt dat Nederland met de alomvattende benadering van de nota internationaal voorop loopt. Dit maakt een effectieve inbreng vanuit Nederland mogelijk.

Waar het gaat om internationale regulering is het mondiale niveau het meest ideaal. Een goed alternatief vormt de kring van westerse landen, waarbij ik dan in de eerste plaats denk aan de landen van de OESO. Ook de Raad van Europa is een geschikt niveau, zeker waar aan de werkzaamheden van de Raad van Europa ook wordt deelgenomen door een aantal belangrijke niet-Europese landen, zoals de Verenigde Staten.

Het is natuurlijk wel zo dat de marges internationaal vrij smal zijn. Het is niet eenvoudig om vanuit Nederland internationale (en zeker mondiale) besluitvorming in gang te zetten. Ik noem daar nog bij dat op het terrein van de elektronische snelweg de Verenigde Staten een aanzienlijke (kennis-)voorsprong hebben. Een klein land als Nederland kan daar maar in beperkte mate iets tegenover stellen. Dit ligt anders indien in EU-verband consensus bestaat over de te volgen lijn. De totstandkoming van de richtlijn over de juridische aspecten van elektronisch zakendoen heeft onder meer om die reden voor mij hoge prioriteit. Die richtlijn moet de basis gaan vormen voor een Europese rechtsontwikkeling op dit terrein.

Een andere vraag is welke rol nog voor de nationale wetgever overblijft. Ik ben van oordeel dat de nationale wetgever in ieder geval moet zeker stellen dat fundamentele waarden en normen worden beschermd. Dit behoort tot de kern van de nationale rechtsstaat, een rechtsstaat waar nog steeds behoefte aan bestaat en ook zal blijven bestaan.

Daarnaast kan de nationale wetgever een rol spelen bij het faciliteren van elektronisch rechtsverkeer vanaf Nederlands grondgebied. Hiermee kan hij vertrouwen scheppen en daarmee de ontwikkeling van elektronisch

rechtsverkeer in Nederland – en daarmee de concurrentiepositie – bevorderen.

Een en ander neemt niet weg dat (de handhaving van) nationale regelgeving zich slecht verhoudt tot het internationale karakter van de elektronische snelweg. Bij het opstellen van nieuwe regels zal de uitvoerbaarheid en de handhaafbaarheid steeds expliciet moeten worden onderzocht, gelet op dit internationale karakter.

Het vervolg op de nota

Tot slot van deze inleiding ga ik nog in op het vervolg op de nota. Sinds het verschijnen van de nota is bijna een jaar verstreken. In deze periode hebben zich op internationaal terrein een aantal belangrijke ontwikkelingen voorgedaan. Ik schetste die eerder. Op nationaal gebied zijn niet alle termijnen uit het actieplan gehaald. Dit komt onder andere doordat het actieplan zeer ambitieus is opgesteld en de complexiteit van de vraagstukken met zich meebracht dat de geplande termijnen niet altijd haalbaar bleken. Het ambitieuze actieplan van de nota zal dan ook bijstelling behoeven.

Mede in het licht van het voorgaande zie ik voor deze kabinetsperiode de volgende prioriteiten:

1. het instrumentarium op het gebied van strafrecht en strafvordering moet voldoende zijn toegesneden op de elektronische snelweg. Dit geschiedt onder meer via het wetsvoorstel Computercriminaliteit II (actiepunt 2.1 uit de nota). Bovendien wordt een evenwicht gevonden tussen de diverse belangen, die een rol spelen bij encryptie en de rol van Trusted Third Parties daarbij.
2. de juridische infrastructuur wordt verbeterd, ten behoeve van het elektronisch verrichten van rechtshandelingen. Dit geschiedt in de eerste plaats door aanpassing van het Burgerlijk Wetboek (actiepunten 1.1 en 1.2) en de Algemene wet bestuursrecht (actiepunt 4.1).
3. aandacht gaat uit naar de kwaliteit van de publieke dienstverlening, voor zover regelgeving daarbij een rol kan spelen (o.a. ter uitvoering van actiepunten 5.1 en 5.2).
4. de strategie voor de internationale aanpak op dit terrein wordt (verder) ontwikkeld, ter uitvoering van actiepunt 12.3 uit de nota. Veel belang hecht ik daarbij aan de totstandkoming van de EU richtlijn over juridische aspecten van de elektronisch zakendoen.

Vragen 1 en 44

De nota schetst een veelheid aan juridische vraagstukken, die verband houden met de ontwikkeling van de informatiesamenleving. Bij sommige van die vraagstukken kan de technologie ook juridische problemen oplossen. Dit geldt in de eerste plaats in de sfeer van de rechtshandhaving: de technologie biedt niet alleen de mogelijkheid voor burgers om zich aan een rechtshandhavende overheid te onttrekken, maar biedt ook voor de overheid juist ook weer mogelijkheden om sporen na te gaan. Ook op andere onderdelen biedt de technologie mogelijkheden. Zo stelt de nota voor het gebruik van Privacy Enhancing Technologies (PET) te bevorderen, om daarmee een adequate privacybescherming mogelijk te maken. Het thema «betrouwbaarheid» (Deel III D van de nota) rust voor een belangrijk gedeelte op de technologie, die een betrouwbare communicatie juist mogelijk maakt. Dit zal in de toekomst tevens gelden voor elektronische equivalenten voor schriftelijke communicatie; de ontwikkeling daarvan is thans nog onvoldoende om in alle gevallen het schriftelijkheidsvereiste in privaatrechtelijke of bestuursrechtelijke wetgeving te kunnen laten vervallen.

Vraag 2

De Reclame Code Commissie ziet toe op uitingen van reclame. Daarbij is de aard van het medium indifferent. De normen en waarden die hier gelden, zijn ook van toepassing op uitingen van reclame op het Internet.

Vraag 3

De elektronische snelweg is in de nota gebruikt als een metafoor voor een veelheid aan verschijningsvormen van technologieën, systemen, netwerken en toepassingen. De vraag of de elektronische snelweg een openbare ruimte is, is dan ook niet in algemene zin te beantwoorden. Langs de elektronische snelweg vinden vele vormen van communicatie plaats, zowel met een openbaar als met een besloten karakter. Voor de werking van ons recht is onder meer bepalend het onderscheid tussen openbare en besloten communicatie, als ook de vraag of in een bepaald geval informatie eenvoudig toegankelijk is voor een ieder.

Vraag 4

In de algemene inleiding bij de beantwoording ben ik ingegaan op het uitgangspunt «wat «off line» geldt, moet ook «on line» gelden». Hier gaat het om de vraag of ook het omgekeerde een uitgangspunt kan zijn. Het kan zijn dat zich rond het elektronisch domein geheel nieuwe rechtsbeginselen ontwikkelen. Over deze rechtsbeginselen vindt in wetenschappelijke kringen reeds een eerste debat plaats, zo bleek onder meer bij de jaarvergadering van de Nederlandse Juristenvereniging van 12 juni 1998. Te denken valt bijvoorbeeld aan een nieuwe invulling van een recht op anonimiteit of ook aan een recht dat ziet op de authenticiteit of integriteit van communicatie.

Het debat over deze nieuwe beginselen bevindt zich nog in een beginfase. Ik sluit niet uit dat nieuwe te ontwikkelen rechtsbeginselen voor het elektronisch domein ook hun weerslag hebben op het recht dat «off line» geldt. Ik vind het echter te vroeg om daarover nu reeds een standpunt te ontwikkelen. Immers, nieuwe rechtsbeginselen moeten zich eerst wortelen in de samenleving. Wel is het nuttig dat het kabinet het debat over nieuwe rechtsbeginselen stimuleert (zie ook de algemene inleiding).

Vraag 5 en 21

Voorbeelden van verdringing van traditionele middelen van communicatie door middelen van elektronische communicaties zijn:

- de grote, gedrukte encyclopedie wordt vervangen door een elektronische versie;
- verzending van documenten geschiedt niet langer per fax, maar per e-mail;
- telefoneren is niet meer met geld mogelijk, maar alleen nog maar met een chipkaart.

Ik verwijs voor andere voorbeelden naar blz. 30 van de nota.

Vraag 6

Op de bladzijden 63 en 64 van de nota wordt informatie verstrekt over de Model Law on Electronic Commerce van de United Nations Commission on International Trade Law. Ter verduidelijking daarvan moge het volgende dienen. De modelwet is in 1996 door UNCITRAL vastgesteld. Zij is het product van de Working Group on Electronic Commerce van UNCITRAL en is gericht op het totstandbrengen van een technologie-onafhankelijke juridische infrastructuur, waarin het gebruik van het elektronisch rechtsverkeer, als alternatief voor het traditionele mondelinge en papieren rechtsverkeer, geen oneigenlijke voor- of nadelen biedt. Teneinde dit doel van «non-discriminatie» van het elektronisch rechtsverkeer te bereiken, gaat de modelwet uit van de zgn. «functional equivalent approach». Dit houdt in dat voor iedere door het recht opgeworpen, aan de traditionele omgeving ontleende belemmering voor

het elektronisch rechtsverkeer, zoals bijvoorbeeld de eis van een geschrift, moet worden gezien wat daarvan het elektronisch functionele equivalent is, en dat aan het gebruik van dit equivalent in een elektronische omgeving dezelfde rechtsgevolgen worden toegekend als aan het naleven van het desbetreffende (vorm)vereiste in een traditionele omgeving. Voor het vaststellen van het elektronisch functionele equivalent moet eerst worden gezien wat doel en functie van het desbetreffende (vorm)vereiste in de traditionele omgeving zijn en vervolgens op welke wijze dit doel en deze functie in een elektronische omgeving op kwalitatief gelijkwaardige wijze kunnen worden gewaarborgd. Toepassing van deze benadering leidt dus tot het ontwikkelen van «elektronische (vorm)vereisten». Dit heeft het voordeel dat de in de traditionele omgeving door (vorm)vereisten bestreken rechtshandelingen evengoed in elektronische vorm kunnen worden verricht, zonder dat dit hoeft te leiden tot het simpelweg schrappen van deze (vorm)vereisten; die worden immers vrijwel steeds gesteld ter bescherming van een kwetsbaar belang dat anders gemakkelijk in de knel zou raken, zoals de bescherming van consumenten, economisch zwakkeren e.d.

De modelwet is tot dusverre de enige mondiaal totstandgebrachte regeling van de juridische aspecten van elektronisch zakendoen en in die zin dus logischerwijs het enige model waarnaar gekeken is. Het is tevens een regeling die internationaal breed gedragen wordt en ook in een aantal landen reeds in nationale wetgeving is of zal worden verwerkt. In de nota is echter verschillende malen tot uitdrukking gebracht dat de modelwet weliswaar een belangrijke inspiratiebron zal zijn bij het totstandbrengen van enkele algemene bepalingen omtrent het vermogensrechtelijk elektronisch rechtsverkeer in het Burgerlijk Wetboek, maar niet de enige. Ook nationale wetgeving van andere landen en (model)regelgeving ontwikkeld door (internationale) (beroeps)organisaties, alsmede ontwerpen van een en ander, zullen uiteraard in de beschouwing worden betrokken.

Vraag 7

Tot op heden wordt er noch nationaal noch internationaal gewerkt aan het opstellen van specifieke internationaal privaatrechtelijke regels voor Internet. Wel staat het codificeren van dergelijke regels op de agenda van de Haagse Conferentie. De Haagse Conferentie is een gevestigd instituut met als doel de unificatie van het Internationaal Privaatrecht. Zij kent een zittingsperiode van vier jaar, waarin een of meer thema's of projecten worden behandeld. In het jaar 2000 wordt een diplomatieke conferentie worden gehouden, waar het nieuwe programma wordt vastgesteld. Daar zal worden beslist of tot het opstellen van dergelijke regels zal worden overgegaan. De Nederlandse regering acht een hoge prioriteit voor dit onderwerp gewenst. Als het onderwerp hoge prioriteit krijgt, kan in 2004 een verdrag ter tafel van de Haagse Conferentie liggen. Krijgt het onderwerp die prioriteit niet – wat afhankelijk is van de beslissing van een diplomatieke conferentie die in 2000 gehouden zal worden – dan zal Nederland intern met het onderwerp aan de slag gaan (zie ook vraag 38).

Vraag 8

Op de bladzijden 65 tot en met 68 van de nota wordt de problematiek van de privaatrechtelijke aansprakelijkheid van tussenpersonen getoetst aan de bestaande wettelijke regeling van de onrechtmatige daad. Daarbij wordt de conclusie getrokken dat het geldend recht op dit punt voldoende mogelijkheden biedt om tot bevredigende resultaten te komen, zoals het leerstuk van de onrechtmatige daad door de jaren heen in staat is geweest nieuwe maatschappelijke en economische ontwikkelingen op te vangen. Dit heeft voor een belangrijk deel te maken met het feit dat de elementen van het leerstuk op een zodanig hoog abstractieniveau zijn geformuleerd dat zij zonder problemen op alle terreinen van het maatschappelijk leven,

en dus ook in een elektronische omgeving, kunnen worden toegepast. De wettelijke regeling van de onrechtmatige daad is daarmee een schoolvoorbeeld van (reeds bestaande) technologie-onafhankelijke wetgeving. Deze analyse wordt nog steeds onderschreven. Wel valt inmiddels te bezien of dit uitgangspunt zal kunnen worden volgehouden. Immers, op 18 november 1998 heeft de Europese Commissie een ontwerp-richtlijn inzake enkele juridische aspecten van de elektronisch zakendoen aangeboden aan de Raad van de Europese Unie (zie ook de algemene inleiding). In dit ontwerp zijn tevens specifieke bepalingen zijn opgenomen betreffende de (niet-) aansprakelijkheid van tussenpersonen op de elektronische snelweg voor bepaalde typen van activiteiten. Een eerste bespreking van deze richtlijn in het verband van de Raad heeft op 18 december jl. plaatsgevonden.

Vraag 9

Dit onderzoek, zoals opgenomen onder punt 11 van het actieplan, is nog niet ter hand genomen.

Vraag 10

Zoals in de nota aangegeven, heeft het vorige kabinet de lijn gekozen – en het huidige kabinet neemt die lijn over – dat het gebruik van cryptografie vrij behoort te blijven, gelet op de noodzaak daarvan uit een oogpunt van bescherming van de privacy en bevordering van elektronisch zakendoen. Er zijn dan ook geen voornemens om maatregelen te treffen tegen het gebruik van cryptografische technieken. Wel brengt het uitgangspunt dat telecommunicatie aftapbaar moet blijven ten behoeve van de strafvordering, mee dat (juridische) mogelijkheden moeten worden gecreëerd om, in geval van een concrete verdenking dat strafbare feiten worden gepleegd, versleutelingen achteraf ongedaan te maken. Dit heeft ertoe geleid dat in het wetsvoorstel Computercriminaliteit II, dat thans aanhangig is bij de Raad van State, een verplichting is opgenomen voor degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van telecommunicatie, om mee te werken aan de ontsleuteling daarvan. In dit verband beraadt het kabinet zich nog op de positie van Trusted Third Parties in de situatie dat zij betrokken zijn bij de versleuteling van gegevensverkeer en het voor de autoriteiten met het oog op de opsporing van strafbare feiten van belang is hiervan kennis te krijgen.

In het kader van het Wassenaar Arrangement bestaan er wel internationale afspraken omtrent de export van goederen voor tweëerlei gebruik (dwz. goederen bestemd voor twee doeleinden nl. militair en civiel), tot welke categorie ook encryptie behoort. Doel van die afspraken is om een bijdrage te leveren aan de internationale en regionale veiligheid en stabiliteit. De uitvoerregels die daar uit voortvloeien zijn echter niet gericht op het aan banden leggen van het gebruik van dergelijk producten in algemene zin, maar creëren wel de mogelijkheid om te voorkomen dat bepaalde cryptografische producten ongecontroleerd in handen komen van in of vanuit het buitenland opererende terroristische en criminele organisaties of in handen komen van landen die zulke terroristische activiteiten ondersteunen.

Vraag 11

Het begrip «document» in de Wet openbaarheid van bestuur (Wob) is reeds thans niet beperkt tot papieren documenten; het kan onder omstandigheden dus ook elektronische documenten omvatten. Een gelijkstelling van elektronische met schriftelijke documenten in de Wob is overbodig. In artikel 1, onderdeel a, van de Wob is vastgelegd dat onder het begrip document wordt verstaan: een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat. Dat de Wob een ruimer documentbegrip hanteert, houdt verband met de

omstandigheid dat daarin de informatie centraal staat en niet het document. Wel is overigens vereist dat de informatie concreet aanwezig is.

Vragen 12, 28, 69 en 70

In de algemene inleiding bij deze beantwoording ben ik reeds in algemene zin ingegaan op het vraagstuk van zelfregulering.

Hier beantwoord ik de meer specifieke vragen die over dit onderwerp zijn gesteld, waarbij ik mij, net als in de algemene inleiding, steeds richt op zelfregulering als alternatief voor wetgeving. Met andere woorden: zelfregulering als uitvoering van een publieke taak.

De vraag is gesteld naar een voorbeeld van hoe de overheid – als een van de mogelijkheden voor het toezicht op zelfregulering – onvoldoende vertegenwoordigde belangen behartigt. Ik noem als voorbeeld dat overheid betrokken is bij de onderhandelingen voorafgaande aan de totstandkoming van zelfregulering, zoals het geval is bij de gedragscode voor elektronisch zakendoen. Indien bij de totstandkoming van die gedragscode zou blijken dat met het belang van de consument onvoldoende rekening wordt gehouden kan de overheid zich dat belang aantrekken. Dit kan de overheid door er voor te zorgen dat organisaties van consumenten in voldoende mate bij de onderhandelingen over de gedragscode worden betrokken, of, in een bijzonder geval, door zelf het belang van consumenten te verdedigen.

En andere vraag is of de voorkeur voor zelfregulering op de elektronische snelweg als alternatief voor wetgeving niet leidt tot een doorbreking van het adagium «wat «off line» geldt, moet ook «on line» gelden». In de algemene inleiding gaf ik reeds aan dat dit adagium soms leidt tot een nadere invulling voor de elektronische omgeving. In een dergelijk geval geldt de rechtsnorm – bijvoorbeeld een verbod om bepaalde handelingen te verrichten – gelijk voor de «on line» en voor de «off line»-omgeving. De vormgeving van die norm of de invulling van die norm kan dan voor de «on line»-omgeving anders zijn, door daarvoor een voor de elektronische omgeving specifiek instrument te kiezen.

Zo staat bij het opstellen van regels voor een technologisch turbulente «on line»-omgeving flexibiliteit van die regels voorop. Dit leidt tot een sterkere voorkeur voor zelfregulering dan voor de «off line»-omgeving. Overigens wijs ik op Aanwijzing 7, onderdeel c, van de Aanwijzingen voor de regelgeving. Bij het ontwerpen van wetgeving – op welk terrein dan ook – moet steeds worden bezien in hoeverre zelfregulering een geschikt instrument is.

De vragen 12 en 70 zijn reeds in de algemene inleiding beantwoord.

Vraag 13

Ja. De regering is van mening dat bij het voorkomen van strafbare uitingen zelfregulering een nuttige rol kan spelen. Geconstateerd kan worden dat de activiteiten van het door de providers ingestelde Meldpunt Kinderporno in belangrijke mate hebben bijgedragen aan het verkrijgen van inzicht in het opsporen van kinderpornografisch materiaal op Internet. Naast zelfregulering is uiteraard een actieve houding van de politie en Justitie nodig. In zijn brief van 6 augustus jl. heeft de Minister van Justitie aangegeven met welke maatregelen hij de bestrijding van kinderpornografie door politie en OM op een hoger plan wil brengen.

Vraag 14

Terecht wordt aandacht gevraagd voor deze passage in de samenvatting van de nota, waarin twee op de bladzijden 68 tot en met 70 van de nota behandelde onderwerpen zijn ten onrechte samengetrokken. Deze passage moet luiden:

- Er moeten aanvullende regels komen voor de rechtsmacht inzake

- Internet, waarbij prioriteit gegeven moet worden aan internationale rechtsmachtregels.
- Bezien moet worden of het bestaande materiële internationaal privaatrecht met zijn aanknopingspuntenleer voldoende houvast biedt om het toepasselijke recht op rechtsvragen betreffende Internet vast te stellen.

Vraag 15

Onder handhavingsautoriteiten worden de verschillende nationale en internationale opsporingsinstanties verstaan. Er zijn regels over samenwerking tussen dergelijke instanties, vastgelegd in verdragen. Het internationale karakter van de elektronische snelweg – en daarmee het wegvallen van fysieke grenzen – maken het evenwel noodzakelijk om aanvullende regels over samenwerking overeen te komen teneinde adequaat tegen inbreuken op economische ordeningswetgeving, vermogensdelicten en computerdelicten te kunnen optreden.

Vragen 16, 17, 34 en 52

In de algemene inleiding wees ik er reeds op dat de ontwikkelingen in internationaal verband snel gaan en vermeldde ik de diverse internationale organisaties waar gesproken wordt. Met name de OESO-Conferentie in Ottawa van oktober 1998 maakt de lijnen duidelijk waarlangs de internationale gedachtenontwikkeling gaat. Het leek verstandig deze conferentie af te wachten, alvorens concreet invulling te geven aan de pragmatische meersporenaanpak uit de nota.

De resultaten van de OESO-Conferentie zijn vrij globaal, maar geven toch een goede indruk welke onderdelen uit de pragmatische meersporenaanpak internationaal zullen aanslaan en welke niet. Opvallend is dat het mogelijke ontstaan van vrijhavens – landen die zich aan internationale afspraken onttrekken en daardoor een toevluchtsoord worden voor ongewenste activiteiten – internationaal niet als een probleem wordt gezien. Andere onderdelen lijken internationaal meer succesvol te kunnen zijn, met name: zelfregulering als alternatief voor overheidsregulering, afspraken over de uitoefening van rechtsmacht en de samenwerking tussen autoriteiten.

Ik betrek de resultaten van de conferentie bij het werkplan als bedoeld in actiepunt 12.3 van de nota.

Wat betreft de harmonisatie van materiële wetgeving wijs ik op het voorstel van de Europese Commissie van 18 november 1998 voor een richtlijn inzake juridische aspecten van elektronisch zakendoen. Dit voorstel beoogt onder meer de aansprakelijkheid van de Internetprovider binnen de EU te harmoniseren. In de algemene inleiding gaf ik reeds het belang aan dat ik aan dit voorstel hecht. Voor het overige zijn geen concrete voorstellen bekend, voor harmonisatie van materiële normen. In antwoord op de vraag naar de initiatieven van Nederland voor internationale regulering noem ik het naar mijn oordeel belangrijkste voorbeeld. Nederland speelt een initiërende rol bij de totstandkoming van een verdrag over misdrijven in de elektronische omgeving («crime in Cyber-space»). Nederland levert de voorzitter van de deskundigengroep die dit verdrag voorbereidt.

Vraag 18

Het vereiste van dubbele strafbaarheid houdt, in het kader van de internationale strafrechtelijke rechtshulp, in dat een staat in het algemeen alleen tot rechtshulp (bijv. uitlevering of bepaalde onderzoekshandelingen zoals inbeslagneming) ten behoeve van een andere staat zal overgaan indien het delict waarop het verzoek om rechtshulp betrekking heeft, ook naar het eigen recht een strafbaar feit inhoudt. Het is ten onzent onder andere neergelegd in artikel 5, eerste lid, Uitleveringswet, de artikelen 552y, eerste lid, onder b, en 552o, tweede lid, Wetboek van Strafvordering

en artikel 3, eerste lid, onder c, Wet overdracht tenuitvoerlegging strafvonnissen.

Vraag 19

Aangenomen kan worden dat de vraagsteller doelt op het opstellen van een gedragscode als een vorm van zelfregulering. Zoals op de bladzijden 180–182 van de nota aangegeven, wordt in het algemeen en vooralsnog de voorkeur gegeven aan vormen van zelfregulering boven wetgeving. Een gedragscode voor de privaatrechtelijke en strafrechtelijke aansprakelijkheid van tussenpersonen behoort dus wat de regering betreft zeer wel tot de mogelijkheden, zij het dat het initiatief daartoe van het betrokken bedrijfsleven behoort uit te gaan. De overheid kan daarbij op een ondersteunende en faciliterende wijze betrokken zijn.

Er wordt niet gedacht aan het opstellen van overheidswege van een gedragscode voor de strafrechtelijke aansprakelijkheid van tussenpersonen. Gedragscodes moeten totstandkomen in het kader van zelfregulering. Wel is in het eerdergenoemde wetsvoorstel Computercriminaliteit II een regeling van de strafrechtelijke aansprakelijkheid van tussenpersonen opgenomen. Een dergelijke wettelijke regeling kan zelfregulerende activiteiten (bijv. het Meldpunt kinderporno) ondersteunen en verder richting geven.

Op internationaal niveau kan gewezen worden op het voorstel van de Europese Commissie van 18 november 1998 voor een richtlijn inzake de juridische aspecten van elektronisch zakendoen waarin onder andere gepoogd wordt de aansprakelijkheid van de Internetprovider binnen de EU te harmoniseren (zie ook het antwoord op vraag 17).

Vraag 20

Openbare registers zijn van groot maatschappelijk belang. Ze bevatten echter ook informatie die vertrouwelijk is verstrekt (bijvoorbeeld bestanden van het CBS), en informatie die betrekking heeft op de persoonlijke levenssfeer. Teneinde legitieme belangen te beschermen is de toegang tot en het gebruik van de onderscheiden registers in specifieke wetgeving vastgelegd. Omdat de condities in die wetten noodzakelijkerwijs onderling verschillen kan over de elektronische toegang tot die registers geen algemene uitspraak worden gedaan. Elke vakminister zal voor de «eigen» bestanden aan moeten geven hoe en wanneer dat geregeld wordt. Een voorbeeld daarvan is de intentie die staatssecretaris Tommel heeft neergelegd in zijn brief aan de Kamer inzake de evaluatie van de verzelfstandiging van het Kadaster. Daarin heeft hij een beleidslijn neergelegd over de publieke elektronische toegang tot de Kadaster gegevens. De openbare overheidsarchieven zijn op dit moment nog vooral in papieren vorm beschikbaar. Die bestanden die elektronisch bij de archiefdiensten beschikbaar zijn kunnen onder de geldende condities van de Archiefwet worden geraadpleegd.

Vraag 21

Zie vraag 5.

Vraag 22

Op basis van artikel 4.1 van de Telecommunicatiewet kan de overheid de toewijzing van Internet namen en adressen naar zich toe trekken. Momenteel vindt deze toewijzing plaats op basis van zelfregulering. Er is vanuit de markt geen signaal ontvangen dat hier zodanige knelpunten zijn dat er noodzaak zou zijn voor de overheid om deze toewijzing naar zich toe te trekken.

Een studie naar een mogelijke rol van de nationale regelgevers (NRA's), onder andere op het vlak van Internet naamgeving en adressering, vindt momenteel plaats op Europees niveau. Deze studie die de ETO (European Telecommunications Office) uitvoert voor de Europese Commissie is nog

in een inventariserend stadium en richt zich ook op mogelijke knelpunten rond toewijzing van Internet namen en adressen. Het eerste resultaat van de studie indiceert dat er geen noodzaak lijkt te zijn voor een overheidsbemoeienis.

De Nederlandse overheid volgt dit terrein nauwgezet. Bij de behandeling van dit vraagstuk dient een verschil te worden gemaakt tussen het beheer van het aan Nederland toebedeelde landencode-domein (ccTLD) met de aanduiding «.nl» («het «.nl» domein») en de generieke domeinnamen van het hoogste niveau («gTLDs»).

Het beheer over het «.nl» domein wordt sinds 1996 gevoerd door de op initiatief van een aantal providers opgerichte Stichting Internet Domeinregistratie Nederland.

De nota stelt op blz. 152 dat het huidige stelsel naar tevredenheid in een aantal publieke belangen voorziet, en dat het erop zal toezien dat dit stelsel blijft voldoen aan de eisen voor zelfregulering, zoals uiteengezet in Deel IV van de nota. Om voor een transparante besluitvorming te zorgen heeft de Stichting op 9 juni 1998 in de Beurs van Berlage een congres gehouden over het door haar bij het toebedelen van domeinnamen gevoerde beleid. Uit de uitkomsten van dit congres blijkt dat niet alleen de betrokken industrie, maar ook het bij Internet betrokken maatschappelijk veld tevreden is over deze gang van zaken en over de in het Reglement van de Stichting gehanteerde criteria. Op een aantal punten heeft de Stichting overigens in de uitkomsten van het congres aanleiding gezien om het Reglement op korte termijn iets te versoepelen. Uit het voorgaande blijkt duidelijk dat dit stelsel, met de ingebouwde mogelijkheden van terugkoppeling, een goed voorbeeld is van effectieve zelfregulering. Op dit moment zie ik derhalve geen aanleiding om overheidsinterventie aan de orde te stellen.

Voor de gTLDs is de situatie als volgt. Het beheer van Internet zal worden overgedragen aan een private onderneming, die door een raad van bestuur wordt geleid waarin vertegenwoordigers van alle werelddelen zitting zullen hebben (ook een vertegenwoordiger namens Nederland). Ook hier zal vooralsnog sprake zijn van zelfregulering. Nederland houdt dit proces verder bij door middel van inbreng naar de Europese Commissie, die op dit terrein namens de Europese Gemeenschap met de Amerikaanse overheid onderhandelt, en door actieve deelname aan bijeenkomsten van de WIPO, waar een procedure wordt uitgewerkt voor de beslechting van geschillen die bij de aanvraag van een nieuwe domeinnaam voor een gTLD zouden kunnen ontstaan.

Vraag 23

Op datamining zijn de regels zoals neergelegd in het voorstel voor een Wet bescherming persoonsgegevens onverkort van toepassing. Dit betekent onder andere dat datamining door de politie slechts mag plaatsvinden voor zover dat noodzakelijk is voor de goede vervulling van haar taak en dat de vergaarde gegevens – behoudens wettelijke uitzonderingen – slechts mogen worden gebruikt voor het doel waarvoor ze zijn vergaard.

Het onderzoek naar datamining is begrepen in het onderzoek «meewerken aan strafvordering». Dit is een meerjarig onderzoek. Er is voorzien in deelrapportages. De eerste deelrapportage is in de loop van 1999 te verwachten.

Regels voor het zogenaamde verkennend onderzoek (het «branche-onderzoek») zijn voorzien in het wetsvoorstel bijzondere opsporingsbevoegdheden (kamerstukken II 1996/97, 25 403). De officier van justitie zal in het kader van een dergelijk onderzoek tevens kunnen bepalen dat gegevens worden vergaard uit bepaalde openbare registers. Het is de bedoeling dat het openbaar ministerie in zijn jaarverslag steeds verantwoording zal afleggen over het gebruik van deze specifieke bevoegdheid tot datamining.

Vraag 24 en 25

Door de Raad van Europa is een Committee of Experts on Crime in Cyber-space (PC-CY) ingesteld met als opdracht een veelomvattend internationaal verdrag ter zake van de bestrijding van grensoverschrijdende computercriminaliteit voor te bereiden. Naar mijn mening is dit een belangwekkend initiatief, mede omdat ook landen als de Verenigde Staten en Canada (als waarnemers) bij de voorbereiding betrokken zijn en zich dus waarschijnlijk ook zullen aansluiten bij het verdrag. In het verdrag zullen zowel materieelrechtelijke bepalingen worden opgenomen – ter harmonisatie van nationale strafbepalingen op het terrein van computercriminaliteit – als speciale rechtshulpprocedures, die er met name op gericht zijn snel optreden op computernetwerken mogelijk te maken.

De werkzaamheden van de werkgroep zijn momenteel in volle gang. Naar verwachting zal eind 1999 een ontwerp tekst gereed zijn, waarna de gebruikelijke besluitvormingsprocedure kan starten. Nederland speelt bij de totstandkoming van dit (ontwerp)verdrag een actieve rol. Nederland levert de voorzitter van de werkgroep van de PC-CY die is belast met het ontwerpen van de verdragsteksten.

Vraag 26

Een richtlijn van de Europese Unie inzake de elektronische handtekening is in voorbereiding. In deze richtlijn wordt geregeld dat een elektronische handtekening onder bepaalde voorwaarden in juridisch opzicht gelijk gesteld wordt met een handgeplaatste handtekening. Op deze wijze wordt ernaar gestreefd het gebruik van elektronische handtekeningen en derhalve ook het elektronisch rechtsverkeer binnen de Unie te stimuleren. Hierbij zij aangetekend dat de richtlijn geen betrekking heeft op rechtshandelingen waarvoor in het nationale recht van de lidstaten vormvereisten gelden, zoals bijvoorbeeld een notariële akte. Dit soort rechtshandelingen valt buiten het kader van de richtlijn en blijft beheerst worden door het nationale recht. In EU-verband hebben de afgelopen maanden onderhandelingen plaatsgevonden over de ontwerp-richtlijn. Er is echter nog geen gemeenschappelijk standpunt bereikt.

Wellicht ten overvloede kan nog worden opgemerkt dat ook op nationaal niveau zal worden voorzien in wetgeving die relevant is voor de erkenning van elektronische handtekeningen maar niet uitsluitend daarop is gericht. Dit is in de nota aangekondigd en vloeit mede voort uit de aanbevelingen van de interdepartementale werkgroep «elektronisch verrichten van rechtshandelingen» die in het kader van de operatie Marktwerving, Deregulering en Wetgevingskwaliteit (MDW) heeft onderzocht in hoeverre vormvereisten een belemmering vormen voor het verrichten van rechtshandelingen op de elektronische snelweg. Wat betreft de nota kan worden gewezen op het op bladzijde 63 beargumenteerde voornemen een beperkt aantal algemene bepalingen in het Burgerlijk Wetboek op te nemen, die ertoe strekken de rechter enkele leidende beginselen te bieden bij de toepassing van het burgerlijk recht op de elektronische snelweg. Daarbij zal vooropstaan het beginsel dat het langs elektronische weg verrichten van rechtshandelingen in beginsel geen oneigenlijke voor- of nadelen behoort op te leveren ten opzichte van het gebruik van de traditionele mondelinge of schriftelijke weg. Hiermee volgt Nederland de modelwet van UNCITRAL (zie ook het antwoord op vraag 6).

In het MDW-rapport wordt dit voornemen overigens als «experimentele wetgeving» of «experimenteerbepalingen» aangeduid. Deze betiteling blijkt verwarring op te leveren. Ik spreek dan ook niet langer over het experimentele karakter: het gaat om normale in Boek 3 van het Burgerlijk Wetboek op te nemen wettelijke bepalingen, die derhalve in beginsel zullen gelden voor al het vermogensrechtelijk elektronisch rechtsverkeer. Verder wordt overeenkomstig de aanbevelingen van de MDW-werkgroep een wetsvoorstel voorbereid, dat het mogelijk maakt voor een consument

om elektronisch een koop van een onroerende zaak aan te gaan, waarbij hem ter bescherming tegen o.a. overijling een bedenktijd wordt gegeven.

Vraag 27

Allereerst is gedacht aan het opnemen van algemene bepalingen in het Burgerlijk Wetboek (zie het antwoord op vraag 26). Deze bepalingen strekken er onder meer toe een impuls te geven aan de mogelijkheden voor een betrouwbaar elektronisch rechtsverkeer dat in, vanuit of naar Nederland plaatsvindt. Dit moet het voor partijen interessant maken in, vanuit of naar Nederland elektronisch zakendoen te drijven.

Daarnaast is ook de liberalisatie van de telecommunicatie een belangrijk voorbeeld. Nederland heeft door deze liberalisatie versneld in de Telecommunicatiewet vast te leggen een voorsprong behaald.

Ook kan nog worden gedacht aan regelgeving die bepaalde stimulansen op fiscaal terrein geeft, zoals op basis van de Wet bevordering speur- en ontwikkelingswerk gebeurt.

Uiteraard zal de Nederlandse wetgever steeds rekening moeten houden met het Europese recht. De bepalingen in het Burgerlijk Wetboek mogen niet in strijd komen met de in voorbereiding zijnde richtlijnen op het gebied van de elektronische handtekening (zie het antwoord op vraag 26) en terzake juridische aspecten van de elektronische handel (zie o.a. de algemene inleiding). De Telecommunicatiewet is in belangrijke mate een uitvoering van de Europese telecommunicatiewetgeving.

Verder gelden uiteraard steeds de vier vrijheden uit het EG-verdrag en het Europees mededingingskader, dat met name voor de liberalisatie van de Telecommunicatiesector van belang is.

De fiscale faciliteiten worden bij de Europese Commissie aangemeld op grond van de artikelen 92 en 93 van het EG-verdrag (Staatssteun).

Vraag 28

Zie onder vraag 12 c.a.

Vraag 29, 72, 73 en 74

Geconstateerd wordt dat er sprake is van een ambitieus actieplan ter zake van de wetgeving voor de elektronische snelweg. Dat is ook het geval. Daarbij speelde de notie dat het actieplan, en zeker een aantal elementen daaruit, nodig was in verband met maatschappelijke ontwikkelingen op het terrein van de elektronische snelweg.

In het regeerakkoord wordt aangegeven dat het Nationaal Actieprogramma Elektronische Snelwegen (NAP) verder vorm wordt gegeven; de implementatie van de nota valt daaronder. In de algemene inleiding heb ik uiteengezet welke keuzes daarin spelen en welke accenten ik leg. Het actieplan zelf noemt enkele speerpunten. Deze zijn de projecten 1.1: opnemings van algemene bepalingen in het BW (en het daaraan gerelateerde project 1.2: (opheffing concreet gebleken wettelijke belemmeringen voor het elektronisch wegverkeer)), 2.1 (indiening wetsvoorstel Computercriminaliteit II), 9.1 (ondersteuning van de totstandkoming van Trusted Third Parties met faciliterende wetgeving) en 12 (de problematiek van de internationale rechtsmacht). Deze projecten zijn alle in gang gezet. Met de voorbereiding van een bepaling in het Burgerlijk Wetboek is een start gemaakt. Het wetsvoorstel Computercriminaliteit II is in oktober 1998 voor advies verzonden naar de Raad van State. Voor de problematiek van internationalisering en rechtsmacht zijn niet op korte termijn al resultaten te melden; dat hangt samen met en tevens af van lopende internationale ontwikkelingen.

Ten aanzien van andere actiepunten geldt dat op sommige onderdelen concrete tussenstanden vallen te vermelden. Zo is opdracht verleend aan een onderzoeksbureau voor het onderzoek naar aard, ernst en omvang van de ICT-criminaliteit en het gebruik van opsporingsbevoegdheden (3.2) en zijn diverse onderzoeken opgenomen in de onderzoeksprogrammering

van het WODC (2.4, 2.6, 2.7, 12.3). Aangaande de algemene maatregel van bestuur waarin een centraal informatiepunt voor het verkrijgen van abonneegegevens ten behoeve van het bevoegd tappen is geregeld, is inmiddels advies van de Raad van State verkregen. De beleidsnota inzake organisatie, opleiding en uitrusting van de politie (3.3) is inmiddels gereed. Met het oog op de aanpassing van de Grondwet aan het digitale tijdperk wordt een adviescommissie ingesteld.

De voorbereidingen voor een brede zelfreguleringsorganisatie op het terrein van de media verkeren thans in een vergevorderd stadium. Voor video kan de nieuwe opzet in de eerste helft van 1999 operationeel worden. Voor film en televisie kan dit volledig gerealiseerd worden na het aanpassen van het wettelijk kader.

Het onderzoek in opdracht van de Europese Commissie op het terrein van betere controle door ouders zal naar verwachting in de eerste helft van 1999 gereed komen. Dan zal worden bezien of, en zo ja hoe in Nederland daaraan een vervolg kan worden gegeven.

Er is derhalve veel in gang gezet. Niettemin kan ik een zekere scepsis welke uit de vragen blijkt wel invoelen. De termijnen die in het actieplan zijn genoemd, zijn niet alle gehaald. Aan de hand van de bespreking in Uw Kamer en mede gelet op andere wensen die op het terrein van de wetgeving bestaan, zal een realistischer planning noodzakelijk zijn.

Vraag 30 en 31

De nota beschrijft drie stadia van ontwikkeling van de elektronische snelweg, te weten het stadium van luxegoed, van nevenschikking en van verdringing. De passage in de nota waar de vragensteller op wijst, ziet op het eerste stadium. De klassieke media – de pers in zijn diverse verschijningsvormen, radio en open televisiekanalen – zijn thans van groot belang vanwege de lage toegangsdrempel voor deze media en de forum-functie die zij mede daardoor in de samenleving vervullen. De positie van deze media is tevens van belang omdat zij thans de verankering vormen van een pluriforme informatievoorziening en cultuurverspreiding met een betrouwbare kwaliteit. In overeenstemming met het uitgangspunt van deze nota, is het te vroeg uitspraken te doen over de situatie in mogelijke volgende stadia.

Vraag 32

Internet en andere elektronische diensten zijn steeds minder in de categorie «Luxegoed» te plaatsen. Deze ontwikkeling vindt in belangrijke mate in de markt plaats. Voor een doorbraak op nog grotere schaal zijn met name voorzieningen voor veilige transacties (betalen, autorisatie) nodig. De overheid bevordert deze voorzieningen in het kader van het NAP.

Het aantal Internet gebruikers binnen Nederland stijgt nog steeds snel (eind april 1998 had 8% van de Nederlandse bevolking toegang tot Internet, een verdubbeling ten opzichte een jaar daarvoor*; in mei had 11% van de Nederlandse huishoudens al toegang tot Internet, nu is dat al 16%. Daar komt het zakelijk gebruik nog bij. Een percentage van 15% wordt beschouwd als voldoende kritische massa). Redenen voor deze snelle stijging zijn dat steeds meer kabel-TV aanbieders ook Internet toegang aanbieden aan hun klanten en dat de tarieven van Internet Service Providers nog steeds dalen. Daarnaast nemen steeds meer mensen op hun werk of anderszins kennis van Internet en daarop aangeboden diensten, waardoor zij worden gemotiveerd om ook zelf een aansluiting te nemen. Een voorbeeld hiervan is dat steeds meer bibliotheken steeds vaker Internet toegang aanbieden aan hun bezoekers. Op termijn is het de verwachting, zeker op de transatlantische verbindingen, dat Internet verkeer veel meer bandbreedte in beslag zal nemen dan het normale telefoonverkeer.

Categorieën van gebruikers van Internet en andere elektronische diensten

* Bron: Nipo, 20 april 1998.

zijn steeds minder gemakkelijk te benoemen. Ging het tot voor kort vooral om studenten en hoger opgeleiden, nu zien we dat andere groepen in onze samenleving hun weg naar Internet weten te vinden (om een voorbeeld te geven: de snelst groeiende groep onder de Internet gebruikers is die in de leeftijdscategorie 35–64). Dit wordt veroorzaakt door de hiervoor omschreven ontwikkelingen, maar ook door de vlucht die e-mail neemt. E-mail wordt steeds meer gezien als een gemakkelijk en goedkoop middel om in contact te blijven met bijvoorbeeld familie en vrienden die in een ander land leven.

Vraag 33

Wettelijke termen als «bezit», «voorhanden hebben» of het in het Wetboek van Strafrecht gebruikte «in voorraad hebben» (zie de artikelen 132, eerste lid, 137e, eerste lid, onder 2, en 240b Sr) moeten worden uitgelegd in het licht van de context waarin ze worden toegepast (i.c. een openbaar computernetwerk) en mede gelet op het doel van de desbetreffende wettelijke bepaling. Wat het strafrecht betreft, kan men stellen dat de genoemde termen een zekere (feitelijke) beschikkingsmacht veronderstellen. Dit betekent dat de enkele aansluiting op Internet niet impliceert het bezit van alle uitingen die op het net voorkomen. Voor bezit is mijns inziens ten minste vereist dat de betrokkene een uiting van Internet haalt naar zijn computer en op min of meer duurzame wijze vastlegt (bijv. door haar op te slaan op de harde schijf).

Ook wat het burgerlijk recht betreft, duidt het begrip bezit op het uitoefenen van feitelijke macht, zij het het uitoefenen van macht voor zichzelf; dat wil zeggen met de pretentie van het zijn van rechthebbende.

Vraag 34

Zie vraag 16.

Vraag 35

Sinds de jaren '80 zijn de sturingspretenties van overheden steeds minder geworden. Om die reden benoemt het regeerakkoord economische dynamiek – en als invulling daarvan het poldermodel – als een van de belangrijkste drijfveren van onze samenleving. Dit verschijnsel van een terugtrekkende overheid geldt te sterker voor een terrein als het onderhavige, waar de ontwikkelingen zeer snel gaan en vaak onvoorspelbaar zijn. Bij de ontwikkeling naar een informatiesamenleving lopen marktpartijen voorop. De overheid zal de voorwaarden moeten scheppen om die ontwikkeling mogelijk te maken, maar zal niet zelf voor die ontwikkeling zorg dragen.

Internationaal zou overigens ook geen draagvlak te vinden zijn voor een andere aanpak. Bij de twee grote ministersconferenties die over dit onderwerp zijn gehouden – in juli 1997 in Bonn en in oktober 1998 in Ottawa, onder auspiciën van de Europese Commissie, respectievelijk de OESO – bleek er communis opinio te bestaan onder de westerse landen over een aanpak waarbij marktpartijen leidend zijn. De overheid bepaalt wel de randvoorwaarden.

Vraag 36

Het kabinet zal binnenkort een notitie naar de Kamer zenden, waarin haar visie ten aanzien van de totstandkoming van een TTP-infrastructuur is opgenomen. Hierbij zal aandacht worden besteed aan de verschillende – en vaak tegengestelde – belangen die bij de totstandkoming van TTP's een rol spelen.

Het bedrijfsleven is op dit moment in overleg met o.m. de overheid bezig om deze infrastructuur in de praktijk gestalte te geven (zie antwoord op vraag 63).

TTP's zullen in een vrije markt tot stand komen. In de praktijk zien we al een aantal organisaties die diensten op dit gebied aanbieden of

voornemens zijn dit te doen. Het beleid van de overheid is gericht op het stimuleren van deze ontwikkeling. Daarnaast stimuleert de overheid tevens het tot stand komen van zelfregulering, die onder meer moet waarborgen dat deze organisaties ook daadwerkelijk betrouwbaar en veilig opereren. Bij zelfregulering kan worden gedacht aan een accreditatie- en certificatiestructuur. Een dergelijke structuur heeft ook in andere sectoren bewezen succesvol te kunnen zijn.

TTP's kunnen een groot aantal diensten aanbieden. Op dit moment lijkt de belangrijkste daarvan de elektronische handtekening te zijn (identificatie en authenticatie). Via een betrouwbare toepassing van encryptietechnieken kunnen TTP's wellicht ook diensten aanbieden ter bevordering van de privacy- en eigendomsbescherming. Of deze diensten ook daadwerkelijk zullen worden aangeboden is in eerste instantie een kwestie van vraag en aanbod.

Vraag 37

De huidige wettelijke omschrijving van hetgeen een toerekenbare onrechtmatige daad oplevert, wordt niet gewijzigd met het oog op de elektronische snelweg.

Wel is het volgende onderscheid van belang. De criteria van het leerstuk van de onrechtmatige daad betreffen het materiële recht en zijn dusdanig abstract geformuleerd dat zij zonder bijzondere problemen toepasbaar zijn op de elektronische snelweg. De handhaafbaarheid daarvan staat los van deze materieelrechtelijke kwestie, maar hangt af van de mate waarin in de praktijk bewijsbaar zal zijn dat aan de criteria is voldaan en – in het verlengde daarvan – van de mate waarin op de elektronische snelweg de naleving van bijvoorbeeld een rechterlijk verbod of bevel feitelijk kan worden afgedwongen. Het is niet goed mogelijk problemen van handhaafbaarheid op te lossen louter door het herformuleren van de materieelrechtelijke criteria voor aansprakelijkheid. Daarbij komt dat op dit moment nog niet valt vast te stellen of de handhaafbaarheid een probleem zal gaan vormen. Om die reden bestaat er thans geen aanleiding om op dit moment de regeling van de onrechtmatige daad met het oog op de elektronische snelweg te herformuleren.

Vraag 38

Zowel nationaal en internationaal wordt – in het bijzonder in wetenschappelijke publikaties en wetenschappelijke bijeenkomsten – gezocht naar het in kaart brengen van en het vinden van oplossingsrichtingen voor internationale problemen inzake Internet. Bij de Haagse Conferentie zal worden aangedrongen om dit onderwerp een hoge prioriteit op het werkprogramma van de Conferentie te geven (zie het antwoord op vraag 7).

Vraag 39

De stelling op bladzijde 70 van de nota dat de algemene begrippen van het vermogensrecht in het Burgerlijk Wetboek technologie-onafhankelijk zijn, is gebaseerd op de analyse daarvan, zoals beschreven op de bladzijden 59 tot en met 61. Aldaar worden enkele kernbegrippen van het vermogensrecht onderzocht met het oog op de vraag of zij in de weg staan aan elektronisch rechtsverkeer. De conclusie luidt dat deze kernbegrippen van het vermogensrecht niet aan elektronisch vermogensrechtelijk rechtsverkeer in de weg staan, voornamelijk door het feit dat zij ook in de traditionele omgeving toepasbaar moeten zijn op een grote diversiteit van situaties en omstandigheden en derhalve alle op een hoog abstractieniveau zijn geformuleerd. Voor zover bekend bestaat over deze conclusie in wetenschap en praktijk ook geen wezenlijk verschil van inzicht.

De vraag of deze begrippen handhaafbaar zijn, komt op een andere plaats in de nota aan de orde, te weten onder «Rechtshandhaving», op

bladzijden 163 tot en met 166. Aldaar wordt getracht – het betreft hier een onontgonnen terrein – de handhaafbaarheid van het vermogensrecht in grote lijnen in kaart te brengen, waarbij de conclusie luidt dat vooralsnog voldoende mogelijkheden tot handhaving lijken te bestaan.

In de nota wordt voorts op bladzijde 167–168 gesteld dat, mocht dat niet het geval zijn, moet worden overwogen een algemene wettelijke regeling betreffende middelen tot bewaring van rechten in een elektronische omgeving onder te brengen in het Wetboek van Burgerlijke Rechtsvordering. Daarvoor zullen de ontwikkelingen in de praktijk moeten worden afgewacht. Op dit moment zijn mij geen voorbeelden bekend waarin van een zodanige onvoldoende werking is gebleken.

Vraag 40

Uit de evaluatie van de Awb is inderdaad gebleken dat bij veel bestuursorganen – anders dan de vraag veronderstelt, zeker niet uitsluitend bij de lagere overheden – de tijdigheid van de besluitvorming tekortschiet. Daaruit kunnen op zichzelf geen conclusies worden getrokken over het bij die bestuursorganen al dan niet aanwezig zijn van deskundigheid op het gebied van elektronisch berichtenverkeer. Niettemin is aannemelijk dat deze deskundigheid niet bij alle bestuursorganen in dezelfde mate aanwezig is. Juist daarom kan niet worden volstaan met een eenvoudige gelijkstelling van elektronische rechtshandelingen aan schriftelijke, maar is het raadzaam daaraan nadere voorwaarden te verbinden.

Vraag 41

Er bestaat nog maar weinig ervaring met het elektronisch verrichten van rechtshandelingen door bestuursorganen. Bovendien gaan de technologische ontwikkelingen als bekend zeer snel. Onder die omstandigheden is onzeker of het in dit stadium reeds mogelijk of verstandig is algemene voorschriften te formuleren. Daarbij ware te bedenken dat deze voorschriften – op straffe van vrijwel onmiddellijke veroudering – «technologie-onafhankelijk» zouden moeten zijn. Gelet hierop is vooralsnog gekozen voor een experimenteer-bepaling, op grond waarvan bestuursorganen die dat willen eerst enige ervaring kunnen opdoen.

Vraag 42

Voor de algemene vragen betreffende zelfregulering verwijs ik naar de inleiding en mijn antwoord op vraag 12 c.a.

Wat de strafrechtelijke aansprakelijkheid van Internet Service Providers betreft, merk ik op dat door adequate zelfregulering providers invulling kunnen geven aan de verantwoordelijkheid die zij op grond van de strafwet hebben en onder omstandigheden kunnen voorkomen dat zij door middel van strafvervolging aansprakelijk worden gesteld voor bijvoorbeeld de verspreiding van strafbare uitingen. Uiteraard kan zelfregulering op dit vlak nooit wettelijke aansprakelijkheid vervangen (Zie ook vraag 17 over het richtlijnvoorstel van de Europese Commissie over onder andere de aansprakelijkheid van providers).

Vraag 43

Gebleken is dat de in het Wetboek van Strafrecht opgenomen strafbepalingen vooralsnog voldoende technologie-onafhankelijk zijn geformuleerd zodat ze ook strafbare gedragingen in de elektronische omgeving omvatten. Het vereiste van een technologie-onafhankelijke formulering is voorts vooral van belang bij de omschrijving van strafvorderlijke bevoegdheden. Een te zeer op een bepaalde techniek toegespitste omschrijving (bijv. het aftappen van «telefonie» in plaats van «telecommunicatie») kan in een veranderende technologische omgeving een belemmering gaan vormen voor de opsporing van strafbare feiten. Anderzijds moet er uit een oogpunt van handhaafbaarheid voor worden gewaakt dat bevoegdheden niet zo abstract worden omschreven dat

opsporingsambtenaren, officieren van justitie en rechters bij de toepassing in de praktijk onvoldoende houvast hebben. Bij de behandeling van het wetsvoorstel Computercriminaliteit II zal Uw Kamer kunnen nagaan of aan deze noties voldoende recht is gedaan.

Vraag 44

Zie vraag 1.

Vraag 45

Bij de totstandkoming van artikel 350a Sr (en de culpose variant in artikel 350b), strafbaarstellende de «vernieling» van computergegevens, is primair gedacht aan de gegevensverwerking binnen één computer, met name aan daarin opgeslagen gegevens. Nu inmiddels gegevensoverdracht via computernetwerken een grote vlucht heeft genomen en het (wederrechtelijk) wijzigen van dergelijke «stromende» gegevens technisch mogelijk is, is het mijns inziens wenselijk om buiten twijfel te stellen dat de artikelen 350a en 350b Sr ook strekken tot bescherming van stromende gegevens. Een daartoe strekkende wijziging is opgenomen in het wetsvoorstel Computercriminaliteit II.

Vraag 46

Het richtlijnvoorstel ligt thans voor advies bij het Europees Parlement, dat verwacht het advies in januari 1999 te kunnen vaststellen. Daarna zal het voorstel verder worden behandeld door de Raad. Verwacht wordt dat een gemeenschappelijk standpunt nog in de eerste helft van 1999 onder Duits Voorzitterschap tot stand kan komen.

Vraag 47 en 68

Zeer onlangs is in de drie beraden (Korpsbeheerdersberaad, Hoofdofficierenberaad en Raad van Hoofdcommissarissen) de besluitvorming over het Nationaal Actieprogramma Digitaal Rechercheren afgerond. Het actieprogramma behelst voorstellen over de organisatie en opleiding in het kader van het digitaal Rechercheren. Met politie en openbaar ministerie wordt thans gesproken over de uitvoering – waaronder de financiering – van het programma. Het actieprogramma is als bijlage bijgevoegd.

Vraag 48

Met de totstandkoming van de nieuwe Telecommunicatiewet is de liberalisering van de telecommunicatiemarkt in Nederland een feit. Het algemene uitgangspunt daarbij is dat, binnen de daartoe geldende voorwaarden, zoveel mogelijk ruimte gelaten wordt voor initiatieven in de markt. Echter, ook in een geliberaliseerde omgeving heeft de overheid de taak ervoor te zorgen dat iedereen in Nederland een bepaald basispakket aan telecommunicatiediensten en daarmee samenhangende voorzieningen tot zijn of haar beschikking heeft tegen een betaalbare prijs en van een bepaalde kwaliteit. In de Telecommunicatiewet zijn waarborgen vastgelegd voor de regeling van deze zogenoemde universele dienstverlening. In een op artikel 9.1 van deze wet gebaseerde algemene maatregel van bestuur worden de volgende universele dienstvoorzieningen aangewezen:

- het bieden van een aansluiting op het vaste openbare telefoonnetwerk en toegang tot de vaste openbare telefoondienst, alsmede het ter beschikking stellen van
- openbare betaaltelefoons
- telefoongidsen
- abonnee-informatiedienst.

De invulling van dit basispakket is aan evolutie onderhevig. Zodra andere diensten van onmisbaar maatschappelijk belang worden geacht en de vrije markt hierin niet of in onvoldoende mate voorziet, kan – in overeenstemming met de terzake geldende Europese regels – overwogen worden

deze op te nemen in het basispakket van de universele dienst. Op dit moment worden diensten als Internet en mobiele telefonie in een concurrerende markt geleverd. Gezien de aard van deze diensten en de prijsstelling ervan bestaat op dit moment geen aanleiding om deze op te nemen in het basispakket.

Vraag 49

De Telecommunicatiewet bepaalt in artikel 13.1 dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar mogen stellen aan gebruikers indien deze aftapbaar zijn. Dit is de uitwerking van het aftapbeleid dat in mei 1996 door het kabinet met de Tweede Kamer is besproken (kamerstukken 1995/1996, 24 679 nr. 1).

Artikel 13.6, eerste lid, Telecommunicatiewet bepaalt dat de investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die door de aanbieders van openbare telecommunicatienetwerken en -diensten zijn of worden gemaakt teneinde te kunnen voldoen aan de artikelen 13.1, 13.4 en 13.5 te hunner laste komen. Ingevolge artikel 13.6 lid 2 komen de kosten voor de uitvoering van een concrete taplast ten laste van de overheid.

De Staatssecretaris van Verkeer en Waterstaat is verantwoordelijk voor de uitvoering van de Telecommunicatiewet.

Voldoende aandacht voor technisch-commerciële ontwikkelingen op telecommunicatiegebied op nationaal – en in toenemende mate op Europees – niveau blijft hard nodig. Het vroegtijdig meenemen van aftapvereisten in het standaardisatieproces van telecommunicatiesystemen maakt dat het aftappen technisch mogelijk blijft en voorkomt inspanningen en meerkosten achteraf. Door standaardisatie kan adequaat worden ingespeeld op de technologische ontwikkelingen en kunnen de kosten in de hand worden gehouden.

Vraag 50 en 51

Het onderzoek naar de mogelijkheden tot aanpassing van artikel 7 van de Grondwet is een van de onderwerpen die in handen wordt gegeven van de binnenkort in te stellen Commissie grondrechten in het digitale tijdperk (zie de brief van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties van 15 december 1998), die tot taak krijgt voorstellen te doen tot aanpassing van de Grondwet aan de elektronische omgeving. Naar verwachting zal deze Commissie in februari 1999 haar werkzaamheden aanvangen. Tegen de achtergrond hiervan kan thans nog niet worden aangegeven of het mogelijk zal zijn artikel 7 geheel technologie-onafhankelijk te maken.

Vraag 52

Zie vraag 16.

Vraag 53

Ik noem twee belangrijke voorbeelden van internationale zelfregulering:

- Binnen de ICC (International Chamber of Commerce) is een code voor elektronische handel tot stand gekomen.
- De opzet van het beheer van de top level domeinnamen op Internet wordt internationaal langs de weg van zelfregulering vorm gegeven (zie antwoord op vraag 22).

Vraag 54

Het adagium «wat «off line» geldt, moet ook «on line» gelden» heb ik in de algemene inleiding reeds uitvoerig besproken. Daarbij bleek dat het adagium niet steeds vanzelf werkt en dat de overheid zich soms zal moeten inspannen teneinde normen ook op de elektronische snelweg te

kunnen handhaven. Het mondiale karakter van Internet vormt daarbij het meest belangrijke probleem. De nota stelt om die reden een pragmatische meersporenaanpak voor.

Wat betreft de concrete vraag over de toepasbaarheid van het Nederlands recht bij elektronisch zakendoen wijs ik er op dat de toepasbaarheid van recht wordt bepaald door de regels van het internationaal privaatrecht. Het Nederlands recht is in dat kader toepasbaar, bijvoorbeeld wanneer de aanbieder of de afnemer in Nederland gevestigd is. Probleem is dat op transacties over Internet vaak meer rechtsstelsels tegelijk toepasbaar zijn, waardoor onzekerheid bestaat over de vraag welke materiële rechtsregels nu gelden. Een oplossing daarvoor is het harmoniseren van rechtsregels voor elektronisch zakendoen. De modelwet van UNCITRAL vormt daarvoor een belangrijke aanzet. Verder spant het kabinet zich in om in het kader van de Haagse Conferentie voorrangregels vast te stellen voor de rechtsmacht van staten (zie ook de vragen 7 en 38).

Vraag 55

Zie vraag 7 en 38.

Vraag 56

Wat betreft de bescherming van persoonsgegevens op de elektronische snelweg doet de overheid meer dan voorlichting, het stimuleren van harmonisatie van internationale normen en het stimuleren van zelfregulering. Met de voorgestelde Wet bescherming persoonsgegevens (Wbp) wordt een – ook voor de elektronische snelweg toereikend – kader gegeven waarbinnen besluitvorming over en concrete maatregelen voor de bescherming van de privacy kunnen plaatsvinden. Zelfregulering is daarbij een belangrijk instrument om de algemene normen van de Wbp te concretiseren voor een bepaalde maatschappelijke sector. Als voorbeeld van voorlichting van overheidswege en stimulering van zelfregulering kan overigens worden gewezen op een in de Raad van Europa voorbereid ontwerp van Richtsnoeren voor de bescherming van de privacy op Internet, waarvan ik een exemplaar ter informatie bijvoeg.

In de algemene inleiding ben ik uitvoerig ingegaan op de omvang van de overheidsverantwoordelijkheid, die ertoe kan leiden dat vanwege het bijzondere karakter van de elektronische snelweg de overheid zich daar terughoudender opstelt dan «off-line» het geval is. Daarbij gaf ik ook aan dat voor een terughoudende opstelling van de overheid geen aanleiding is op terreinen waar fundamentele waarden en normen in het geding zijn. De bescherming van persoonsgegevens is zo'n terrein.

Overigens ben ik van mening dat de overheid in beginsel dient te respecteren dat burgers zich anoniem op de digitale snelweg begeven, net als in het «normale» verkeer. Dit neemt niet weg dat in bijzondere situaties, wanneer er een redelijk vermoeden is dat strafbare feiten worden gepleegd, er mogelijkheden moeten zijn om iemand achteraf te traceren, bijvoorbeeld via een Internet Service Provider. Een dergelijke traceerbaarheid via de Internet Service Provider is een van de elementen van de aansprakelijkheidsregeling voor tussenpersonen zoals opgenomen in het wetsvoorstel Computercriminaliteit II.

Vraag 57

De stand van zaken met betrekking tot verificatie van personen met behulp van biometrie (hieronder worden niet begrepen de traditionele pasfoto en de gewone handtekening) is, dat wel sprake is van een toenemend aantal plannen en een beperkt aantal pilots (vaak nog in een voorbereidingsfase), maar dat het aantal operationele toepassingen nog zeer beperkt is. Voorzover mij bekend, gaat het daarbij in vrijwel alle gevallen om z.g. gepersonaliseerde biometrie.

Er is sprake van een grote verscheidenheid van biometrische technieken die in specifieke toepassingssituaties steeds verschillende voor- en

nadelen opleveren. Gelet op de geringe toepassing in Nederland wordt vooralsnog afgewacht hoe zich internationaal de de facto (technische) standaardisatie voltrekt. Internationale afspraken moeten uiteindelijk het juiste kader bieden. Standaardisatie pleegt daarbij in internationale samenwerking door privaatrechtelijke organisaties tot stand te worden gebracht (zelfregulering).

Het kabinet heeft zich in de nota uitgesproken voor stimulering van anonieme vormen van biometrische persoonsverificatie, ook binnen de overheid. Vanuit privacy oogpunt is dit een verantwoorde koers. Extra wetgeving is daar niet voor nodig. Dat neemt niet weg, dat binnen de overheid behoefte lijkt te bestaan aan een algemene wettelijk basis voor het gebruik van biometrie door de overheid zelf, vooral ook om daarmee het gebruik van biometrie door de overheid te bevorderen en eventuele onduidelijkheden over wat wel of niet mag, weg te nemen. Daarnaast wens ik een nadere wettelijke regeling voor opslag en gebruik van gepersonaliseerde biometrische gegevens in breder EU-verband, vooral voor biometrische gegevens waaruit lichaamskenmerken kunnen worden afgelezen of waarmee die lichaamskenmerken kunnen worden gereconstrueerd (teruggerekend). Aangezien verspreiding en gebruik van deze biometrische persoonsgegevens zich niet storen aan landsgrenzen, is nationale regelgeving in principe geen afdoende middel.

Vraag 58

Nog daargelaten de praktische haalbaarheid hiervan, ben ik geen voorstander van het instellen van een algehele identificatie- en registratieplicht bij het betreden van de elektronische snelweg. Zoals de vragers terecht opmerken geldt een dergelijke plicht in de «fysieke» wereld immers ook niet. Voor het vraagstuk van privacy en traceerbaarheid op de elektronische snelweg verwijs ik verder naar het antwoord op vraag 56.

Vraag 59

Het een (een of meer centrale aanspreekpunten) kan heel wel naast het ander (per bedrijf, orgaan of organisatie een privacyfunctionaris) bestaan. Zij kunnen elkaar ook aanvullen. Zo bepaalt artikel 63, derde lid, van de voorgestelde Wet bescherming persoonsgegevens dat privacyfunctionarissen moeten worden aangemeld bij de Registratiekamer en dat deze laatste een lijst bijhoudt van de aangemelde functionarissen. Met vragen over de bescherming van zijn persoonsgegevens kan de burger dus altijd bij de Registratiekamer terecht. Zo nodig kan deze hem dan doorverwijzen naar een terzake deskundige privacyfunctionaris.

Vraag 60

Onder het huidige strafrecht geniet e-mail reeds grotendeels bescherming: voor zover de e-mail in transport is, gelden aftapverboden (zie de artikelen 139c en 374bis Sr), voor zover e-mail is opgeslagen in een computer geldt de strafbaarstelling van computervredebreek (art. 138a Sr). Slechts op enkele onderdelen behoeft die bescherming nog aanvulling. Het bij de Raad van State aanhangige wetsvoorstel Computercriminaliteit II bevat daartoe enkele wijzigingsvoorstellen. Onder andere wordt voorgesteld artikel 125i Sv zo aan te passen dat voor het justitieel onderzoek van e-mail dezelfde (strikte) eisen gelden als voor het onderzoek van poststukken.

Wat de handhaafbaarheid van de strafrechtelijke bescherming van e-mail betreft, verdient opmerking dat niet altijd duidelijk zal zijn dat iemand een e-mail bericht bestemd voor een ander zonder diens toestemming heeft geopend. In zo'n geval is sanctionering van de onbevoegde inzage niet eenvoudig. Gelet hierop verdient de huidige praktijk, waarin gebruikers van e-mail hun e-mailbox doorgaans hebben beveiligd (bijvoorbeeld door middel van een password), krachtige ondersteuning. Verder wijs ik erop

dat een belangrijke waarborg voor de handhaving van de eisen die gelden voor het strafvorderlijk onderzoek van e-mail, is gelegen in het vereiste toezicht van de rechter-commissaris.

Vraag 61

Het millenniumprobleem leert dat het falen van de techniek een dusdanige invloed kan hebben op de maatschappij en de economie dat het tot de taak van de overheid gaat behoren om hier actief op te treden. Daarbij blijft de primaire verantwoordelijkheid uiteraard bij de direct betrokkenen liggen.

Vraag 62

Het functioneren van de samenleving, en dus ook van de overheid, is in belangrijke mate afhankelijk van het goed functioneren van digitale technieken. Op vergelijkbare wijze is de samenleving overigens afhankelijk van de beschikbaarheid van bijvoorbeeld fossiele brandstoffen of elektriciteit. Deze afhankelijkheid is geen probleem als de continuïteit van de betreffende voorziening voldoende kan worden gewaarborgd. Dit vergt voortdurende aandacht. Het millenniumprobleem is daar een voorbeeld van.

Vraag 63

Op dit moment wordt door het betrokken bedrijfsleven in overleg met de overheid en de Consumentenbond gewerkt aan het tot stand brengen van een betrouwbare, veilige en interoperabele TTP-infrastructuur in Nederland. In dat kader wordt met name gezien aan welke eisen TTP's in de praktijk moeten voldoen, en welke structuur nodig is om de toepassing van deze eisen te controleren. Gelet op de positieve ervaringen met andere intermediaire organisaties wordt daarbij in eerste instantie gedacht aan een accreditatie- en certificatiestructuur waarbij de eindverantwoordelijkheid ten aanzien van de controle bij een onafhankelijke partij ligt. In dit uitwerkingstraject wordt tevens gezien welke rol de overheid hierbij moet spelen. De overheid ziet er in ieder geval op toe dat de verschillende bij de totstandkoming van TTP's betrokken belangen voldoende worden behartigd (zie ook het antwoord op vraag 36).

Vraag 20a

Zoals in deel III van de nota aangegeven, staan de overheid verschillende instrumenten ten dienste om, wanneer dit noodzakelijk blijkt, de toegankelijkheid en pluriformiteit bij de informatievoorziening te garanderen. Voorop staat echter dat de overheid bevordert dat in de maatschappij door middel van haar georganiseerde verbanden – bedrijven, verenigingen, maatschappelijke organisaties, e.d. – een toegankelijke en pluriforme informatievoorziening tot stand komt. Daarbij richt de overheid zich in het bijzonder op het voorkomen van ongewenste machtsconcentraties op dit terrein. Onder meer doet thans de Adviescommissie Cross-ownership onderzoek naar de mate waarin netwerken van bedrijven een dergelijke machtsconcentratie vormen en naar de wenselijkheid dit met wettelijke maatregelen tegen te gaan.

Vraag 64

Op openbare overheidsinformatie mag geen monopolie bestaan. Op 8 mei 1998 heeft de minister-president een aanwijzing vastgesteld inzake «het verrichten van marktactiviteiten door organisaties binnen de rijksdienst» (Stcrt 8 mei 1998, nr. 95).

Aanwijzing 13, lid 2, luidt als volgt:

«Gegevens die zijn verkregen bij het uitvoeren van een overheidsstaak en waarvan het gebruik voor marktactiviteiten is toegestaan, moeten onder gelijke voorwaarden beschikbaar zijn voor derden.» De zinsnede «waarvan het gebruik voor marktactiviteiten is toegestaan» heeft

betrekking op lid 1 van hetzelfde artikel dat ingaat op openbaarheid van de informatie als noodzakelijke randvoorwaarde voor marktactiviteiten. In de toelichting bij artikel 13 wordt nog opgemerkt: «De aanwijzing regelt dat derden op non-discriminatoire wijze toegang tot deze gegevens hebben, indien zij verkregen zijn bij de uitvoering van een overheidstaak.» Deze aanwijzing beoogt het ontstaan van monopolies, bij een goed functionerende markt, tegen te gaan. Uiteraard zijn marktactiviteiten alleen aan de orde voor overheidsinformatie die conform de bestaande wet- en regelgeving openbaar is.

ICT biedt inderdaad uitgelezen mogelijkheden om de verplichting tot actieve openbaarmaking conform artikel 8 van de Wet openbaarheid van bestuur meer inhoud te geven. In het Actieprogramma Elektronische Overheid dat het kabinet min of meer gelijktijdig met de beantwoording van deze vragen uitbrengt, worden acties aangekondigd die tot een grotere toegankelijkheid zullen leiden.

Vraag 65

Het onderscheid tussen transport en opslag is met name voor het strafrecht van belang.

In het strafrecht dient voorop te staan dat het legaliteitsbeginsel eist dat zowel strafbepalingen als strafvorderlijke bevoegdheden zo nauwkeurig mogelijk worden omschreven. Reeds hierom ben ik geen voorstander van het loslaten van het onderscheid tussen situaties waarin sprake is van opslag van gegevens in computers en situaties waarin gegevens «onderweg» zijn van A naar B (ook al is er wellicht in technische zin sprake van opslag op tussenstation C). Ik meen daarbij dat het door het gebruik van een weloverwogen en voor de «gebruikers» van de wet inzichtelijke terminologie goed mogelijk is dit onderscheid in de wetgeving te handhaven. De wetgever zal per situatie moeten bezien wat hij strafbaar wil stellen dan wel waartoe hij een opsporingsambtenaar bevoegd wil maken en daarop zijn terminologie moeten afstemmen. Dit heeft in het meergenoemde wetsvoorstel Computercriminaliteit II geleid tot enkele terminologische aanpassingen. Bij de behandeling daarvan zal ik nader ingaan op het onderscheid en op de daarbij te hanteren criteria.

Vraag 66

Het behoeft nauwelijks betoog dat de genoemde uitgangspunten in bepaalde situaties tot een zekere spanning kunnen leiden tussen de verschillende beschermde belangen (respectievelijk de door strafbepalingen beschermde belangen, de belangen van verdachten en getuigen, het belang van een vrije markt en het financieel belang van de burger). Er zal dus steeds naar een evenwicht in de handhaving moeten worden gezocht, zowel op wetgevend als op uitvoerend niveau, waarbij sprake is van een evenredige verhouding tussen de beoogde effecten van een bepaalde maatregel en de kosten (in de zin van schade aan bepaalde belangen) ervan. Deze evenredigheidstoets ligt overigens reeds in de omschrijving van het tweede tot en met vierde uitgangspunt besloten. In dit opzicht is het eerste uitgangspunt – wat «off-line» strafbaar is, moet ook «on-line» strafbaar zijn – van een andere orde. Vooral nog kan ik mij geen omstandigheden indenken die een uitzondering op dit uitgangspunt rechtvaardigen, mede gelet op het fundamentele belang van de rechtsge-
lijkheid.

Vraag 67

Een algemene verplichting voor Internet Service Providers om ten behoeve van de opsporing van strafbare feiten bij te houden welke handelingen hun abonnees verrichten bestaat naar huidig recht niet en acht ik ook voor de toekomst onwenselijk. Slechts in geval van een redelijk vermoeden van een ernstig strafbaar feit kan een aanbieder van een telecommunicatiedienst, zoals een Internet Service Provider, worden

verplicht om bepaalde inlichtingen (de zgn. verkeersgegevens) te verstrekken ter zake van verkeer dat door gebruikmaking van zijn dienst heeft plaatsgevonden of plaatsvindt (art. 125f Sv). Dit kan echter alleen indien het vermoeden bestaat dat de verdachte eraan heeft deelgenomen of deelneemt, zodat niet iedere willekeurige, onverdachte burger het risico loopt dat zijn gangen op Internet worden vastgelegd. Ik meen dat ook de voorgestelde Wet bescherming persoonsgegevens – in combinatie met de nieuwe Telecommunicatiewet – op dit punt voldoende bescherming biedt door de eis dat telecommunicatie-aanbieders slechts persoonsgegevens mogen vastleggen voor zover dat noodzakelijk is voor een goede vervulling van hun eigen taak (en niet voor de vervulling van de taak van de politie).

Vraag 68

Zie vraag 47.

Vraag 69 en 70

Zie vraag 12.

Vraag 71

De vaste werkgroep Aanwijzingen voor de regelgeving van de Interdepartementale Commissie voor de Harmonisatie van Wetgeving (ICHW) heeft inmiddels een voorstel voor verankering van het toetsingskader in de Aanwijzingen besproken. Dit voorstel zal worden meegenomen in de vierde wijziging van de Aanwijzingen die nu in voorbereiding is. Naar verwachting zal deze wijziging medio 1999 in werking kunnen treden. De ICHW brengt geen afzonderlijk advies uit over opname van het toetsingskader in de Aanwijzingen.

Vraag 72, 73 en 74

Zie vraag 29.