Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1997–1998

25 880 Wetgeving voor de elektronische snelweg

Nr. 2 **NOTA**

Management Samenvatting

's-Gravenhage, 12 februari 1998

1.	Uitgangspunten	3
2.	Rechtsgebieden	5
3.	Centrale thema's	7
4.	Naar een toetsingskader voor wetgeving	11
5.	Het toetsingskader	12
6.	Implementatie van de nota	14

1. Uitgangspunten

1. De nota beoogt:
- Een legitimatie te geven van het overheidsoptreden tijdens de overgang naar de informatiesamenleving, voor zover het instrument van wetgeving daarbij een rol kan spelen.
- Die legitimatie te concretiseren in een toetsingskader voor de wetgever.
- Op belangrijke onderdelen aan te geven wat de verschillen zijn tussen de fysieke wereld en de elektronische omgeving.
- Voorstellen te doen voor concrete vraagstukken die zich voor doen als gevolg van technologische ontwikkelingen.

De conclusies en voornemens van de nota vormen een bouwsteen bij de herijking van het NAP. De nota houdt rekening met internationale ontwikkelingen: een rechtsvergelijkend onderzoek vormt mede de basis van de nota.

2. Met inachtneming van deze doelstellingen levert de nota de volgende producten op:
- Een gemeenschappelijk kader voor het kabinet, dat houvast biedt bij vragen van wetgeving rond de elektronische snelweg (zie 19 en volgende van deze samenvatting).
- Voorstellen voor het opstellen, aanpassen of intrekken van wetgeving, en voor de inbreng in internationale overlegfora, en daarmee

KST27336
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 1998

samenhangende activiteiten (de belangrijkste voorstellen zijn verwoord in 8 t/m 18 in deze samenvatting).

3. Onderwerp:
- Onderwerp van de nota is de elektronische snelweg, die wordt gezien als het geheel van technische infrastructuren en diensten waarmee verbindingen tot stand worden gebracht, informatie wordt bewerkt, informatie wordt opgeslagen en verspreid. De «elektronische snelweg» is een metafoor voor de overgang naar een informatiesamenleving.
- De elektronische snelweg wordt geconceptualiseerd in drie lagen, die alle drie om een ander optreden van de wetgever kunnen vragen: een netwerk-laag (exploitatie van infrastructuur), een transportlaag (schakel tussen infrastructuur en gebruiker) en een inhoudslaag (toegevoegde waardediensten).
- Er zijn drie niveaus van ontwikkeling van de elektronische snelweg denkbaar: «luxegoed», waarin elektronische diensten een aanvullend en een amusementskarakter hebben, «nevenschikking», waarin elektronische diensten een grote maatschappelijke en economische betekenis hebben, maar waarin geen verdringing van traditionele communicatiemiddelen, de derde variant, optreedt. Bij «verdringing» is het onmogelijk als burger te functioneren zonder toegang te hebben tot de meest voorkomende elektronische infrastructuren en diensten, doordat de traditionele middelen hun betekenis verloren hebben. De nota gaat uit van een niveau van nevenschikking. Daarnaast geeft de nota ook aan wat de taken van de wetgever moeten zijn, indien voor bepaalde diensten een niveau van verdringing is bereikt.

4. Drie aspecten van de geschetste ontwikkelingen vragen in het bijzonder om een nadere plaatsbepaling van de overheid. Dit zijn:
- Dematerialisering: kennis, diensten en informatie die niet in een tastbare vorm zijn neergelegd vormen de motor van de economie. Bij digitale vastlegging is informatie niet meer gebonden aan een bepaalde fysieke drager of plaats. Digitaal vastgelegde informatie is voorts onuitputtelijk, want zij kan oneindig worden gekopieerd, zonder dat dit leidt tot kwaliteitsverlies of vernietiging.
- Internationalisering: De informatiesamenleving is vooral een open samenleving. Informatie is nauwelijks aan plaats en staat gebonden en kan zeer snel doordringen in vele hoeken van de samenleving. Economische en sociale ontwikkelingen zullen nog meer dan in het verleden hun oorsprong vinden in bronnen die buiten het bereik van de nationale overheid liggen.
- Technologische turbulentie: Nieuwe informatietechnieken en -producten volgen elkaar in hoog tempo op, of convergeren tot nieuwe media. De ontwikkeling van de techniek, het maatschappelijk gebruik ervan en de sociale en juridische problemen die erdoor worden opgeroepen, zijn in hoge mate onvoorspelbaar en kennen een hoge omloopsnelheid.

5. Het ontstaan van de informatiesamenleving brengt vergaande veranderingen, maar houdt geen radicale breuk met het verleden in. De centrale rol van de overheid blijft voorlopig beperkt tot ordening. De overheid dient met betrekking tot de elektronische snelweg twee hoofdtaken uit te voeren:
- Waarborgen van een aantal fundamentele waarden en normen in een elektronische omgeving. Hierbij gaat het om de bescherming en regeling van grondrechten, het verzekeren van rechtshandhaving en het bieden van rechtszekerheid.
- Faciliteren van het elektronisch verkeer. Hierbij gaat het om het bevorderen van een transparante en toegankelijke markt, het bevorderen van betrouwbaarheid van het elektronisch verkeer, het

wegnemen van belemmeringen in de bestaande juridische infrastructuur, standaardisatie en het aanbieden of stimuleren van ondersteunende voorzieningen.

Uitgangspunt bij de uitvoering van die taken is, dat de juridische normen uit de fysieke wereld tevens toepasbaar moeten zijn in het elektronische domein: wat «off line» geldt, moet ook «on line» gelden. Het is 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.
Buiten deze twee hoofdtaken heeft de overheid nog een derde taak: het garanderen van een brede toegankelijkheid tot de elementaire voorzieningen die nodig zijn voor het maatschappelijk functioneren van burgers en bedrijven. Deze derde taak leidt nog niet tot de inzet van een juridisch instrumentarium.

6. Mocht in de toekomst op bepaalde terreinen sprake zijn van een niveau van verdringing (zie hiervoor onder 3), dan kan hoogstwaarschijnlijk niet worden volstaan met het vertalen van traditionele normen en kaders. Die zijn immers veelal voor de fysieke wereld ontwikkeld. Dan zal moeten worden overwogen of daarnaast geheel nieuwe normen en kaders nodig zijn. Voorts zal de overheid uitvoering moeten geven aan haar derde taak, door de inzet van juridisch instrumentarium.

7. De nota concludeert dat de bestaande juridische kaders over het algemeen – eventueel na aanpassing – toepasbaar zijn op de elektronische snelweg. Hierbij moet een belangrijke kanttekening worden gemaakt: het internationale karakter van de elektronische snelweg verhoudt zich niet goed met territoriaal georganiseerde overheden. Op de elektronische snelweg spelen fysieke grenzen immers geen rol. De nota concludeert, dat voor dit probleem geen allesomvattende oplossing voorhanden is. Wel is het probleem aanzienlijk te verkleinen door een combinatie van oplossingen. Hiertoe stelt de nota een pragmatische meersporenaanpak voor (zie hierna onder 14), uitgaande van bestaande nationale soevereiniteiten. Vooralsnog moeten de voorgestelde maatregelen voldoende rechtszekerheid scheppen. Het zal van de verdere ontwikkeling van de elektronische snelweg afhangen, of op langere termijn een meer fundamentele aanpak nodig is, waarbij aan deze soevereiniteiten zal moeten worden getornd.

2. Rechtsgebieden

8. De nota behandelt de toepasbaarheid van de drie traditionele rechtsgebieden – het privaatrecht, het bestuursrecht en het strafrecht – op de elektronische snelweg. Daarnaast komen enkele bijzondere rechtsgebieden aan de orde, voor zover zich daar interessante ontwikkelingen voordoen die verband houden met de elektronische snelweg.

9. Het privaatrecht is in belangrijke mate technologie-onafhankelijk geformuleerd en daardoor grotendeels goed toepasbaar op de elektronische snelweg. Zo bestaan voor de totstandkoming van rechtshandelingen in het algemeen geen vormvereisten: zij behoeven niet schriftelijk tot stand te komen. Ook het bewijsrecht werpt in het algemeen geen belemmeringen op.
Voor een aantal rechtshandelingen gelden wel vormvereisten, bijvoorbeeld ter bescherming van de rechtszekerheid of van de zwakkere partij. Het MDW-project «elektronisch verrichten van rechtshandelingen» – waarvan de rapportage in maart 1998 wordt verwacht – beziet in hoeverre deze vormvereisten, die een belemmering kunnen vormen voor het elektronisch rechtsverkeer, kunnen worden aangepast.
Ter bevordering van het elektronisch rechtsverkeer stelt het kabinet voor:

- Algemene bepalingen in het Burgerlijk Wetboek op te nemen. Deze moeten de rechter houvast geven bij de toepassing van het vermogensrecht op de elektronische snelweg. Uitgangspunt daarvoor is onder andere de modelwet van UNCITRAL[1].
- Te bezien of concreet gebleken wettelijke belemmeringen voor elektronisch rechtsverkeer moeten en kunnen worden opgeheven.
- Voor «Trusted Third Parties[2]» een juridisch kader scheppen dat tevens ondersteunend werkt ten opzichte van het materiële recht en het bewijsrecht. Bij het opzetten van dit kader wordt rekening gehouden met de notitie over «Trusted Third Parties» die de ministers van Verkeer en Waterstaat en Economische Zaken in voorbereiding hebben.

Internationale privaatrechtelijke vraagstukken moeten worden opgelost aan de hand van bestaande criteria van het internationaal privaatrecht (ipr). Het opstellen van specifieke ipr-regels, toegesneden op de elektronische snelweg, heeft prioriteit.
Tot slot: het leerstuk van de onrechtmatige daad is in beginsel geschikt voor de elektronische omgeving: een specifieke privaatrechtelijke aansprakelijkheidsregeling voor tussenpersonen – zoals Internetproviders – wordt niet overwogen.

10. Het algemeen deel van het bestuursrecht, dat betrekking heeft op het voorbereiden, verrichten en uitvoeren van besluiten, schrijft op een aantal punten de schriftelijke vorm voor. Deze wettelijke belemmeringen voor de elektronische besluitvorming moeten zo veel mogelijk worden weggenomen, zonder dat dit afbreuk doet aan de rechtszekerheid en de zorgvuldigheid van de besluitvorming. Gelet op de snelle technologische ontwikkelingen, is het nog niet goed mogelijk invulling te geven aan de eisen waaraan elektronische besluitvorming moet voldoen. De nota stelt voor in de Algemene wet bestuursrecht een experimenteerbepaling op te nemen, waarin elektronische documenten onder voorwaarden gelijk kunnen worden gesteld aan schriftelijke documenten. Hiermee krijgen bestuursorganen de mogelijkheid te experimenteren met bijvoorbeeld elektronische vergunningaanvragen.
In het bijzondere deel van het bestuursrecht zijn met name regels voor (de handel in) goederen en diensten van belang. Te denken valt aan regels over gokken, of over het aanbieden van medicijnen. De elektronische handel maakt het buitenlandse aanbieders eenvoudig mogelijk om rechtstreeks goederen of diensten aan te bieden en daarmee vergunningvereisten in de nationale of Europese wetgeving te omzeilen. Waar zich dit voordoet, zal in de wetgeving een specifieke voorziening moeten worden opgenomen, gericht op aanbieders buiten de Europese Unie. Deze aanbieders moet worden verplicht in de Europese Unie een vertegenwoordiger aan te wijzen. Via deze vertegenwoordiger kunnen vergunningvereisten worden geëffectueerd. Over de implicaties van dit voorstel vindt nog nader onderzoek plaats, alsmede een toetsing van de verenigbaarheid van het voorstel met (toekomstige) regelgeving van de Europese Unie en de WTO.

11. Het materiële strafrecht is in belangrijke mate technologie-onafhankelijk geformuleerd. Dit maakt het in het algemeen goed toepasbaar op de elektronische snelweg.
- Een belangrijk uitgangspunt voor de formulering van strafbepalingen is, dat eigendom van elektronische informatie niet goed denkbaar is: digitaal opgeslagen informatie is immers onbeperkt kopieerbaar en daarmee niet uniek. Het strafrecht moet zich dan ook niet op de informatie zelf richten, maar bescherming bieden tegen de inbreuk op technische voorzieningen die rond informatie zijn aangebracht, bijvoorbeeld in de vorm van encryptie.
- De dematerialisering en de internationalisering scheppen behoefte aan

[1] UN Commission on International Trade Law: Model Law on electronic commerce, 1996.
[2] Vertrouwelijke toegevoegde waardediensten, die bijvoorbeeld de echtheid van een electronische handtekening garanderen.

een goede regeling van de aansprakelijkheid van tussenpersonen – zoals Internetproviders – voor illegale informatie die door hun tussenkomst wordt verspreid. Immers, het is vaak moeilijk buiten de tussenpersoon om de dader te achterhalen, laat staan te bestraffen. Daarnaast is ook voor de tussenpersoon duidelijkheid gewenst omtrent de voor hem geldende aansprakelijkheid. Het voorontwerp voor een Wet computercriminaliteit II legt de tussenpersoon de verplichting op om op te treden tegen illegale informatie die door zijn tussenkomst wordt verspreid, en waarvan hij op de hoogte is.
- Voorts moet bij de verdere invulling van de verantwoordelijkheid van de tussenpersoon een belangrijke rol worden toegekend aan zelfregulering. Bijvoorbeeld op een wijze vergelijkbaar met het Internet Meldpunt Kinderporno. Daarbij moet worden gezorgd voor een adequate overheidsondersteuning op het gebied van de wetshandhaving.

Het formele strafrecht is – waar het gaat om opsporingsmogelijkheden op de elektronische snelweg – in beweging. Het Wetsvoorstel bijzondere opsporingsbevoegdheden[1] is bij de Tweede Kamer in behandeling; de Wet computercriminaliteit II, waarvan het voorontwerp in januari 1998 in consultatie is gegaan, regelt enige specifieke aangelegenheden voor de elektronische snelweg.
Het Wetboek van Strafvordering moet een duidelijk onderscheid maken tussen:
- Bevoegdheden ten aanzien van bestaande en toekomstige gegevens. Opsporing gericht op toekomstige gegevens – te denken valt aan het aftappen van draadloze telefoonverbindingen – moet aan termijnen worden gebonden.
- Het elektronisch zoeken op individu en op onbepaalde groepen van personen – het zogeheten «datamining». Bij datamining moeten beperkingen aan de opsporing worden gesteld.

Daarnaast doet de nota nog enkele voorstellen voor technische aanpassingen van het strafrecht.

12. De nota behandelt verder de ontwikkelingen op een aantal bijzondere rechtsgebieden. De volgende springen het meest in het oog:
- Op het gebied van de media is veel aandacht voor de bescherming van jeugdigen. Maatregelen moeten zo veel mogelijk via zelfregulering en in Europees verband tot stand komen.
- Artikel 7 van de Grondwet zal worden aangepast aan de technologische ontwikkelingen.
- De hanteerbaarheid van technische onderscheidingen in de nieuwe Telecommunicatiewet op langere termijn moet worden onderzocht.
- Het auteursrecht is over het algemeen goed hanteerbaar op de elektronische snelweg. Twijfels bestaan over het gebruik van collectieve oplossingen voor het gebruik van nieuwe media – het zogeheten «reprorecht».

3. Centrale thema's

13. In de nota staan vijf thema's centraal. Het eerste thema beziet het meest fundamentele vraagstuk waarvoor de elektronische omgeving de wetgever stelt: internationalisering en rechtsmacht (zie hiervoor onder 7). De volgende drie thema's zijn inhoudelijk van aard en geven de beleidsdoelstellingen aan voor overheidsbemoeienis met de informatiesamenleving: het mogelijk maken van betrouwbaar verkeer tussen burgers, het waarborgen van privacy en het zorgdragen voor een goede werking van de informatiemarkt waartoe burgers toegang hebben. Het vijfde thema beschouwt het sluitstuk van wetgeving, de handhaving van het recht.

[1] IIK 25 403.

14. Het thema «internationalisering en rechtsmacht» houdt het lastigste probleem in dat de elektronische snelweg oproept: de territoriaal georganiseerde overheden en de wereldwijde elektronische snelweg (zie hiervoor onder 7) zijn moeilijk verenigbaar. In de elektronische omgeving hebben fysieke afstanden en staatkundige grenzen veel minder betekenis. De plaats waar iemand zich bevindt, is niet meer automatisch gelijk aan de plaats waar die handelingen worden verricht. Sterker nog: soms is die plaats helemaal niet te lokaliseren.
Voor dit probleem wordt geen allesomvattende oplossing gevonden. De nota komt met een pragmatische aanpak, die uitgaat van:
- een wezenlijk verschil met de pre-elektronische situatie,
- het internationale karakter van het probleem, wat de speelruimte voor Nederland beperkt.

Deze meersporenaanpak omvat de volgende elementen:
- Internationale harmonisatie van materiële normen verdient aanbeveling waar zij kansrijk is, zoals in het privaatrecht en bij economische ordeningswetgeving, vermogensdelicten en specifieke computerdelicten.
- Ook voor andere wetgeving, die vaak is gebaseerd is op culturele verschillen, zoals uitingsdelicten, wordt harmonisatie niet op voorhand afgewezen.
- Er moeten regels komen voor de omvang van de rechtsmacht, waarbij een prioriteit wordt afgesproken over de uitoefening van rechtsmacht. De «aanknopingspuntenleer» uit het bestaande internationaal privaatrecht kan daarbij een rol spelen.
- Er moeten regels komen over de samenwerking tussen handhavingsautoriteiten.
- De mogelijkheid moet bestaan om onder voorwaarden af te zien van het vereiste van dubbele strafbaarheid, thans voorwaarde voor internationale strafrechtelijke samenwerking.
- Een goede internationale regeling van de privaatrechtelijke en strafrechtelijke aansprakelijkheid van tussenpersonen is wenselijk. Voor het strafrecht kan de oplossing van de Wet Computercriminaliteit II (zie hiervoor onder 11) als voorbeeld in het internationaal overleg worden ingebracht.
- Internationale zelfregulering, die sluitend en handhaafbaar is en de nodige waarborgen bevat, moet worden gestimuleerd. Zelfregulering voor satellietcommunicatie en een gedragscode voor informatieaanbieders hebben voorrang.

Een mondiale regeling heeft in alle gevallen de voorkeur. Dit kan onder andere voor het vermogensrecht en het recht op intellectuele eigendom haalbaar zijn. Vaak zal een mondiale regeling echter niet haalbaar zijn. Dan kunnen afspraken tussen geïndustrialiseerde landen, bijvoorbeeld binnen de OESO, of de Raad van Europa, een aanvaardbaar alternatief vormen. Soms zal moeten worden volstaan met regelgeving op het niveau van de Europese Unie.

15. De bescherming van persoonsgegevens – het eerste onderdeel van het thema «privacy» – is onderwerp van de Wet bescherming persoonsgegevens, die in februari 1998 bij de Tweede Kamer wordt ingediend. Deze wet dient ter implementatie van een EU-richtlijn. Ook de ontwerp-Telecommunicatiewet stelt regels met betrekking tot persoonsgegevens voor de sector telecommunicatie. Uitgaande van deze wetsvoorstellen zal het kabinet zich vooral inspannen voor:
- De bevordering van de transparantie van gegevensverwerking voor de burger.
- Het door zelfregulering invullen van de algemene normen van de wet.
- Internationale harmonisatie ook buiten de Europese Unie, in ieder geval in OESO-landen.

Het gebruik van biometrische gegevens – het tweede onderdeel van dit

thema – staat in relatie tot artikel 11 van de Grondwet (onaantastbaarheid van het menselijk lichaam). Dit betekent dat voor dit gebruik:
- Een wettelijke basis nodig is.
- Toestemming van de betrokkene nodig is.

De bescherming van communicatie met een besloten karakter – het derde onderdeel – wordt gedomineerd door artikel 13 van de Grondwet, waarvoor op 21 januari 1998 een wijzigingsvoorstel[1] in de Tweede Kamer is aanvaard. Voor de elektronische snelweg gaat de discussie over de vraag of e-mail onder de bescherming valt. De vraag wordt bevestigend beantwoord: E-mail is in de praktijk altijd door middel van een password beveiligd en wordt beschermd door het nieuwe artikel 13. De strafrechtelijke bescherming van e-mail krijgt verder vorm in het voorontwerp voor een Wet computercriminaliteit II. Hierin wordt onder meer voorgesteld:
- Het kennisnemen door internet service providers van bij hen opgeslagen e-mail strafbaar te stellen.
- Aan justitieel onderzoek van e-mail dezelfde eisen te stellen als aan justitieel onderzoek van poststukken.

Anonimiteit op de elektronische snelweg – het vierde onderdeel – is een relatief begrip. Iemand laat immers altijd sporen achter die iets zeggen over zijn persoon, overigens zonder dat daarmee zijn identiteit komt vast te staan. Het kabinet zal, om te voorkomen dat onnodig gegevens over personen bekend worden, het gebruik van «privacy enhancing technologies» bevorderen, onder andere door het geven van voorlichting. Daartegenover staat dat een identificatieplicht moet worden ingesteld voor het gebruik van aan de persoon gekoppelde biometrie (zie hierna onder 16).

16. De zorg voor een betrouwbare technische infrastructuur – onderdeel van het thema «betrouwbaarheid» – berust allereerst bij aanbieders en gebruikers van de elektronische snelweg zelf. Daarbij worden de minimum-eisen in voldoende mate door de nieuwe Telecommunicatiewet bestreken.
Wel dienen duurzaamheidseisen aan het bewaren van documenten te worden geïnventariseerd op hun hanteerbaarheid op de elektronische snelweg.
De zorg voor een betrouwbaar rechtsverkeer ligt in hogere mate bij de overheid. Dit geldt zeker:
- Voor gevallen waarin de burger niet vrij is in zijn keuze om van de elektronische snelweg gebruik te maken (het niveau van verdringing; zie hiervoor onder 3).
- Voor verhoudingen tussen de burger en de overheid zelf, zoals onder meer geregeld in het bestuursrecht.

Die zorg voor een betrouwbaar rechtsverkeer uit zich in een aantal voornemens. Het kabinet zal:
- Onderzoeken of artikel 350a van het Wetboek van Strafrecht aanpassing behoeft om de manipulatie van de elektronische overdracht van gegevens strafbaar te stellen.
- Zelfregulering over misleiding op de elektronische snelweg, in aanvulling op de regels uit het Burgerlijk Wetboek, stimuleren.
- De elektronische toegang tot openbare registers tot stand brengen, overeenkomstig de nota Toegankelijkheid van overheidsinformatie; het privcy risico dat het technisch koppelen van digitale informatie oplevert dient daarbij te worden meegewogen.
- Internationale afspraken over biometrie bevorderen.
- Nader onderzoek verrichten naar de uitgifte van biometrisch beveiligde elektronische identiteitsbewijzen.
- Voorstellen de Wet op de identificatieplicht met het oog op de elektronische identificatie uit te breiden.

«Trusted Third Parties» zijn belangrijk voor een betrouwbaar rechtsverkeer. Bij de oprichting hiervan speelt zelfregulering een centrale rol,

[1] IIK 25 443.

een en ander onverminderd het onder 9 genoemde juridisch kader. Een vorm van overheidstoezicht is wenselijk (in overeenstemming met de onder 9 genoemde notitie van de Ministers van Verkeer en Waterstaat en Economische Zaken).

17. Bij het thema «markten» luidt de conclusie dat informatie- en communicatiemarkten een bijzonder karakter hebben. De snelle technologische ontwikkelingen en de internationalisering, gevoegd bij het feit dat informatie – wezenlijk voor het functioneren van een democratische rechtsstaat – het onderwerp is, vragen om alertheid van de overheid. Immers, het is voor een samenleving van belang dat informatie breed beschikbaar is. De effectiviteit van het nieuwe wettelijk instrumentarium – en het toezicht door NMA en OPTA – zal regelmatig worden beoordeeld. Daarnaast is standaardisatie van technische normen en koppelvlakken voor het functioneren van markten van belang. Het kabinet zal de totstandkoming van zelfregulering bevorderen en daarbij aandacht schenken aan de keuze voor een geschikte publiekrechtelijke waarborg. Zodra een niveau van ontwikkeling van de elektronische snelweg is ontstaan waarbij verdringing plaatsvindt (zie hiervoor onder 3) vergt de toegankelijkheid voor de burger specifieke aandacht. Dit geldt des te sterker indien ook de communicatie tussen overheid en burger in belangrijke mate langs elektronische weg plaats heeft.
Toepassing van het regime van universele dienstverlening op e-mail en Internet is nog niet aan de orde. Wel kan de overheid een rol spelen bij de toewijzing van adressen en domeinnamen op de elektronische snelweg. Transparantie van die toewijzing vergroot de toegankelijkheid. Het kabinet overweegt ondersteuning te geven aan het huidige systeem van zelfregulering door de Stichting Internet Domeinregistratie.
Ook de pluriformiteit vormt op dit moment geen reden voor interventie door de wetgever. Daarbij moet worden opgemerkt dat de anarchistische structuur van Internet juist pluriformiteit genereert. Reden voor interventie kan ontstaan, zodra:
- Nieuwe media de traditionele media verdringen.
- Voor de meningsvorming belangrijke media «achter het modem» verdwijnen.

De technieken convergeren en de mogelijkheden voor het aanbieden van informatie nemen aanzienlijk toe. Deze ontwikkelingen vragen om hernieuwde afstemming van de verschillende regimes – met name Telecommunicatiewet en Mediawet. Over enige jaren zal deze afstemming nogmaals moeten worden bekeken.

18. De rechtshandhaving vormt het vijfde thema. Technologische ontwikkelingen maken de rechtshandhaving moeilijker, maar ze bieden tevens kansen. Bij het toekennen van strafrechtelijke handhavingsbevoegdheden dienen de volgende uitgangspunten te worden afgewogen:
- Effectieve handhaving op de elektronische snelweg staat voorop: de elektronische snelweg mag geen rechtsvrij gebied worden.
- De inbreuk die de handhaving maakt op de privacy van de burger moet zo gering mogelijk zijn.
- De ontwikkeling van de markt moet worden bevorderd. Daarbij moeten zo min mogelijk beperkingen worden opgelegd aan het toelaten en het gebruik van techniek.
- De kosten voor de gebruiker van de elektronische snelweg mogen niet onevenredig hoog zijn.

Meer concreet:
- Het gebruik van cryptografie blijft vrij.
- Er worden maatregelen voorgesteld om het aftappen van telecommunicatie ook in een veranderde telecommunicatiemarkt mogelijk te houden. Dit mag niet leiden tot onevenredige kosten of tot verstoring

van de concurrentieverhoudingen van de telecommunicatieaanbieders.
- Binnen het kader van de Raad van Europa moeten afspraken worden gemaakt over specifieke rechtsmachtvraagstukken voor de opsporing op het Internet.
- Er vindt onderzoek plaats naar het gebruik van datamining als opsporingstechniek.
- De Tweede Kamer zal voor de zomer van 1998 nader worden geïnformeerd over de voornemens op het gebied van de organisatie van politie en justitie met het oog op de strafrechtelijke rechtshandhaving op de elektronische snelweg.

Privaatrechtelijke rechtshandhaving op de elektronische snelweg stelt nieuwe eisen aan het bewijs. Het kabinet is van plan regelgeving over de digitale handtekening tot stand te brengen. Uitgangspunt daarbij is een voorstel voor een EU-richtlijn dat in het voorjaar van 1998 wordt verwacht. Voorts verdient ook het beslagrecht aandacht: dit gaat uit van fysieke goederen waarop eventueel beslag kan worden gelegd. Niettemin biedt het huidige recht aanknopingspunten voor het bewaren van rechten in de elektronische omgeving. Vooralsnog kan de rechtsontwikkeling dan ook aan de rechter worden overgelaten.

4. Naar een toetsingskader voor wetgeving

19. De centrale kenmerken van de elektronische snelweg (zie hiervoor onder 4) stellen de overheid – samengevat – voor de volgende problemen:
Dematerialisering beïnvloedt:
- Transport en opslag: er is geen vanzelfsprekend onderscheid meer, een juridische fictie is nodig.
- Authenticiteit: gegevens kunnen perfect en onbeperkt worden gekopieerd.
- Anonimiteit versus kenbaarheid: kenbaarheid van de wederpartij is een groot goed, maar botst met de wens van anonimiteit en privacy.
- Open en besloten communicatie: er is geen vanzelfsprekend onderscheid meer.

Internationalisering is besproken onder 14, hiervoor. Oplossingen werden aangedragen voor:
- Botsing van rechtsmachten.
- Uiteenlopen van materiële normen
- Moeizame handhaafbaarheid.

Technologische turbulentie heeft gevolgen voor:
- Technologie-afhankelijkheid: door de snelle opeenvolging en convergentie van technieken biedt regelgeving op basis van concrete media of technieken op langere termijn onvoldoende houvast. Dit kan ook leiden tot rechtsongelijkheid tussen het gebruik van oude en nieuwe technieken, en tot discrepanties tussen de on- en off-line communicatie.
- Flexibiliteit: het proces van formele wetgeving vergt zorgvuldige besluitvorming en kan daardoor te lang duren om de omloopsnelheid van problemen te kunnen bijbenen. Wetgeving dreigt reeds te verouderen voor zij het Staatsblad bereikt.
- Doeltreffendheid: het ontbreekt de wetgever vaak aan de technische expertise en het inzicht in de maatschappelijke toepassingen van de techniek om op voorhand terreinen te kunnen reguleren.

20. De nota ontwikkelt voor de wetgever een toetsingskader, dat hierna onder 22 wordt weergegeven. Dit toetsingskader is gericht tot de actoren in het wetgevingsproces. Daaronder vallen mede diegenen die namens Nederland in Europees of internationaal verband onderhandelen over de totstandkoming van wetgeving. Het kader moet hen in staat stellen om consistente afwegingen te maken bij het voorbereiden en opstellen van

regelgeving. Meer in het bijzonder is het toetsingskader gericht op een goede motivering van gemaakte keuzes, vooral waar die afwijken van de in het kader genoemde hoofdregels.
Het toetsingskader heeft geen dwingend karakter en kan dit, gelet op de complexiteit van de te beantwoorden vragen, ook niet hebben. Bovendien is voor sommige vraagstukken niet één specifiek instrument, maar juist een combinatie van de genoemde instrumenten het meest geschikt.

21. Opmerkingen vooraf:
- Het toetsingskader vormt – voor regelgeving die verband houdt met de elektronische snelweg – een verbijzondering van de Aanwijzingen voor de regelgeving (met name aanwijzingen 6 e.v.).
- Aanwijzing 6 stelt: «Tot het totstandbrengen van nieuwe regelingen wordt alleen besloten als de noodzaak daarvan is komen vast te staan». Voor de elektronische snelweg betekent dit dat een regeling uitvoering moet geven aan een hiervoor onder 5 genoemde overheidstaak.
- De drie kenmerken (zie hiervoor onder 4 en 19) leiden tot een sterke voorkeur voor alternatieven voor formele wetgeving. Daar staat tegenover dat het onzekere karakter van de elektronische snelweg in sommige gevallen juist om rechtszekerheid vraagt. Dit dilemma klinkt in alle oplossingen door.
- Technologie-onafhankelijke wetgeving heeft de voorkeur. Hiermee wordt veelal een gelijkheid tussen de «off line-wereld» en de «on line-wereld» bereikt. Ook is technologie-onafhankelijke wetgeving beter bestand tegen de technologische turbulentie. Echter, technologie-afhankelijkheid zal soms juist nodig zijn. Zo zou de behoefte tot rechtszekerheid aanleiding kunnen zijn voor technologie-afhankelijke wetgeving (zie ook hiervoor onder 19).
- Zelfregulering heeft op korte termijn de voorkeur, maar kent ook risico's. De voorkeur voor zelfregulering geldt niet waar fundamentele waarden en normen in de democratische rechtsstaat in het geding zijn. Voorts stelt de nota een aantal eisen aan zelfregulering als alternatief voor overheidsregulering. De overheid waarborgt de naleving van deze eisen.
- Op langere termijn kan er juist wel weer reden zijn voor overheids-regulering. Dit kan het geval zijn, indien:
  – er sprake is van een niveau van ontwikkeling waarbij verdringing plaatsvindt (zie hiervoor onder 3). De overheid dient dan garanties te scheppen voor de toegankelijkheid.
  – de technologische ontwikkelingen in rustiger vaarwater komen, en een periode van stabiliteit aanbreekt. Ter bevordering van de rechtszekerheid zou dan ook codificatie kunnen plaatsvinden van normen die via zelfregulering tot stand zijn gekomen.

5. Het toetsingskader

22. Het toetsingskader ziet er als volgt uit.

1.1 Regelgeving dient bij voorkeur plaats te vinden op mondiaal niveau, of in ieder geval tezamen met zoveel mogelijk landen. Met name het privaatrecht leent zich daarvoor, en voorts standaardisatie en andere regelgeving op het gebied van de economische ordening, maar ook andere onderwerpen waarover de culturele opvattingen niet sterk uiteenlopen.
Indien dit niet haalbaar is, is regeling in kleiner internationaal verband, zoals OESO of Raad van Europa, een goed alternatief. Indien dat alternatief ook niet haalbaar is, wordt gekozen voor het niveau van de Europese Unie.

1.2 Regelgeving op nationaal niveau kan worden overwogen:
- Ter bescherming van normen en waarden.
- Indien regelgeving op internationaal niveau niet haalbaar is, of te lang zou duren.
- Om de concurrentiepositie van Nederland te versterken.
- Als voorbeeld voor de internationale rechtsontwikkeling.

2.1 Als alternatief voor overheidsregulering dient eerst te worden onderzocht of andere oplossingen mogelijk zijn, waarbij vormen van zelfregulering zoveel mogelijk moeten worden gestimuleerd. Dit geldt in ieder geval zolang:
- geen «verdringing» van traditionele communicatie plaatsvindt, en
- er sprake is van technologische turbulentie.

Daarnaast kan voor problemen, veroorzaakt door technologie, in sommige gevallen de technologie zelf ook oplossingen aanreiken. Filtersystemen ter bescherming van jeugdigen tegen ongewenst aanbod zijn hiervan een voorbeeld.

2.2 Deze zelfregulering dient aan de volgende voorwaarden te voldoen:
- De doelgroepen die in het geding zijn, zijn voldoende georganiseerd.
- Er vindt er een gelijkwaardige behartiging plaats van de relevante maatschappelijke belangen.
- Er vindt voldoende binding plaats van alle partijen.
- De handhaving van de afspraken is voldoende verzekerd.

2.3 De overheid draagt zorg voor de naleving van de voorwaarden genoemd onder 2.2. Zij kan daarvoor onder meer de volgende instrumenten gebruiken:
- Het behartigen van onvoldoende vertegenwoordigde belangen.
- Het opstellen van ondersteunende wetgeving.
- Het dreigen met wetgeving, indien de zelfregulering niet aan de voorwaarden voldoet.
- Toezicht.
- Het meewerken aan de handhaving.

2.4 Overheidsoptreden is in ieder geval aan de orde indien fundamentele normen en waarden van de democratische rechtsstaat in het geding zijn. Met betrekking tot de elektronische snelweg kan men daarbij vooral denken aan bescherming van klassieke grondrechten van burgers en aan de preventie en opsporing van ernstige inbreuken op de rechtsorde en de staatsveiligheid.

3.1 Vanwege het turbulente karakter van de ontwikkelingen rond de elektronische snelweg dient het overheidsingrijpen zo flexibel, adequaat en tijdig mogelijk te zijn. Afweging met het belang van de rechtszekerheid vindt plaats.

3.2 Het wordt getoetst of bestaande wettelijke normen voldoende houvast bieden, zodat de rechtsontwikkeling aan de rechter kan worden overgelaten.

3.3 Het wordt getoetst of overheidsoptreden langs bestuurlijke weg kan plaatsvinden. Daarbij kan men denken aan:
- Een voorbeeld als functiegebruiker van de elektronische snelweg.
- Voorlichting.
- Convenanten.

Voor zover dit bestuurlijk optreden de vrijheid van particulieren beperkt, is daarvoor een wettelijke grondslag vereist.

3.4 Het wordt getoetst of een nadere uitwerking van het privaatrecht met het oog op de elektronische snelweg geschikt is, teneinde rechtsonzekerheid in rechtsverhoudingen weg te nemen.

3.5 Indien geen van de voorgaande vormen, of een combinatie daarvan, voldoet, zal het overheidsingrijpen echter plaats dienen te vinden in de vorm van, of binnen het kader van, formele, publiekrechtelijke wetgeving. Daarbij wordt gezocht naar alternatieven voor materiële normen in de wet. De formele wet omvat alleen algemene normen, tenzij:
- Meer specifieke normen nodig zijn om de bescherming van klassieke grondrechten te verzekeren.
- De voorwaarden worden vastgelegd waaronder de overheid op die rechten inbreuk mag maken.

3.6 Getoetst wordt of technologie-onafhankelijke regelgeving mogelijk is. Technologie-onafhankelijke regels zijn niet geschikt:
- Als definitie van de reikwijdte van een regeling.
- Als rechtssubjecten – in verband met de ingewikkelde technologie – juist behoefte hebben aan inzicht in de technologie.
- Als technologie-onafhankelijke regels aan rechtssubjecten onvoldoende houvast zouden bieden over de aard van hun rechten en plichten.
- De voorwaarden worden vastgelegd, waaronder de overheid op die rechten inbreuk mag maken.

De voorkeur voor technologie-onafhankelijke wetgeving kan er toe leiden inhoudelijke normen niet op te nemen in specifieke, technische wetgeving. Ter toelichting: bijvoorbeeld alle regels over privacy worden opgenomen in een algemene privacywet en niet in verschillende op technologie gebaseerde sectorspecifieke wetten.

3.7 Bij de invulling van algemene normen wordt een keuze gemaakt tussen:
- Zelfregulering.
- Overlaten aan de rechter.
- Een AMvB, of een ministeriële regeling.
- Een mengvorm tussen de voorgaande instrumenten.

6. Implementatie van de nota

23. Het toetsingskader dat hierboven is weergegeven, wordt met onmiddellijke ingang toegepast bij de voorbereiding en vaststelling van regelingen en bij de Nederlandse inbreng in internationale overlegfora. Het toetsingskader zal worden verankerd in de Aanwijzingen voor de regelgeving. Ten behoeve van de implementatie zijn de overige voorstellen van de nota geclusterd in een aantal vervolgprojecten die elk afzonderlijk ter hand kunnen worden genomen. De nota voorziet in een voortgangsbewaking van de implementatie, te coördineren door de Minister van Justitie, zo mogelijk binnen het kader van een tweede Nationaal Actieprogramma elektronische snelwegen. Tot slot wordt voorgesteld de nota na twee jaar te actualiseren.

		Blz.
Deel I.	**Inleidend gedeelte**	**19**
A.	**Algemene inleiding**	**21**
1.	Aanleiding voor de nota	21
2.	Probleemstelling	21
3.	Doel van de nota	22
4.	Opzet van de nota	22
5.	Reikwijdte van de nota	23
6.	De plaats van de nota; afstemming met andere activiteiten	23
7.	Rechtvaardiging	24
B.	**Informatiesamenleving en elektronische snelweg**	**25**
1.	Naar de informatiesamenleving	25
2.	De elektronische snelweg	25
3.	Technische ontwikkelingen	26
3.1.	Digitalisering	26
3.2.	Miniaturisering	26
3.3.	Mobiele telecommunicatie	27
3.4.	Opkomst van telematica	27
4.	Ontwikkelingen in gebruik en toepassing	27
4.1.	Convergentie van de technische middelen	27
4.2.	Convergentie in het aanbod	28
5.	Gelaagde telecommunicatiediensten	28
6.	De ontwikkeling van de informatiesamenleving	29
6.1.	Luxegoed	29
6.2.	Consumptiegoed: nevenschikking	29
6.3.	Noodzaak: verdringing	30
7.	De elektronische snelweg in deze nota: kernpunten	30
C.	**Begrippenlijst**	**31**
Deel II	**Verkenningen**	**41**
A.	**Technische verkenning**	**43**
1.	Inleiding	43
2.	Transport en opslag	43
3.	Bestanden van (persoons-)gegevens	44
4.	Telecommunicatienetten	44
5.	Adressering en identiteit	44
6.	Open en besloten communicatie	45
7.	Digitaal-elektronische betrouwbaarheid	45
7.1.	Het kernprobleem: de verhouding tussen kopie en origineel	46
7.2.	Beschikbaarheid van technische middelen	46
7.3.	Presentatiekwaliteit	46
7.4.	Autorisatie, rechtenbeheer en vertrouwelijkheid	47
7.5.	Cryptografie	47
7.6.	Betrouwbare elektronische betaal- en geldsystemen	48
8.	Conclusies en voorstellen	50
B.	**Bestuurskundige verkenning**	**51**
1.	Inleiding	51
2.	De informatiesamenleving	51
3.	De overheid	51
4.	Visies op de overheid in de informatiesamenleving	53
4.1.	De onmachtige overheid	53
4.2.	De actieve overheid	55
4.3.	De ordenende overheid	55
5.	De rol van de overheid in de informatiesamenleving: afweging	57
6.	Conclusies en voorstellen	58
C.	**Juridische verkenningen**	**59**
1.	Privaatrecht	59
1.1.	Inleiding	59
1.2.	Het vermogensrecht	59
1.2.1.	Enkele algemene begrippen van het vermogensrecht	59
1.2.2.	Wettelijke belemmeringen op specifieke punten?	61
1.2.3.	Zijn de wettelijke bepalingen praktisch toepasbaar in een elektronische omgeving?	62
1.2.4.	Stimulering van ontwikkelingen door wetgeving; verband met internationale ontwikkelingen	63
1.3.	Vermogensrechtelijk elektronisch rechtsverkeer en het bewijsrecht	64
1.3.1.	De uitgangspunten van het civiele bewijsrecht	64
1.3.2.	Specifieke belemmeringen	65
1.3.3.	Bewijsovereenkomst	65
1.4.	Privaatrechtelijke aansprakelijkheid van tussenpersonen	65
1.4.1.	Inleiding	65
1.4.2.	Een toerekenbare onrechtmatige daad	66
1.5.	Het internationaal privaatrecht	68
1.5.1.	Inleiding	68
1.5.2.	Toepasselijk recht	68
1.5.3.	Rechtsmacht	69
1.5.4.	Arbitrage	70
1.6.	Conclusies en voorstellen	70
2.	Bestuursrecht	70
2.1.	Inleiding	70
2.2.	Besluitvorming en elektronische communicatie	71
2.2.1.	Inleiding	71
2.2.2.	De schriftelijkheidseis naar huidig recht	71
2.2.3.	Meer mogelijkheden voor elektronische besluitvorming?	73
2.3.	Internationale rechtsmacht	73
2.4.	Conclusies en voorstellen	75
3.	Strafrecht	75
3.1.	Inleiding	75
3.2.	Het materiële strafrecht: algemeen	76
3.2.1.	Functioneren van informatiesystemen.	76
3.2.2.	Vermogensdelicten	77
3.2.3.	Uitingsdelicten	77
3.3.	Het materiële strafrecht: aansprakelijkheid van de provider	78
3.4.	Het formele strafrecht	80
3.4.1.	Bijzondere opsporingsmethoden	80
3.4.2.	Randvoorwaarden	82
3.4.3.	Medewerking van particulieren	84
3.5.	Conclusies en voorstellen	84
3.5.1.	Conclusies materieel strafrecht	85
3.5.2.	Conclusies aansprakelijkheid van de provider	85
3.5.3.	Conclusies formeel strafrecht	85
4.	Bijzondere juridische verkenningen	86
4.1.	Inleiding	86
4.2.	Auteursrecht en naburige rechten	86
4.2.1.	Inleiding	86
4.2.2.	Beïnvloeding door de elektronische snelweg	86
4.2.3.	Initiatieven tot internationale en Europese regelgeving	87
4.2.4.	Betekenis voor de Nederlandse wetgeving	87
4.3.	Bescherming persoonsgegevens	88
4.3.1.	Inleiding	88
4.3.2.	Beïnvloeding door de elektronische snelweg	88
4.3.3.	Initiatieven tot Europese regelgeving	88
4.3.4.	Betekenis voor Nederlandse wetgeving	88
4.4.	Artikel 13 Grondwet: brief-, telefoon- en telegraafgeheim	90
4.4.1.	Inleiding	90
4.4.2.	Het nieuwe artikel 13	91
4.4.3.	E-mail	91
4.5.	Mediarecht	91
4.5.1.	Inleiding	91
4.5.2.	Beïnvloeding door de elektronische snelweg	92
4.5.3.	Initiatieven tot Europese regelgeving	92
4.5.4.	Betekenis voor Nederlandse wetgeving	93
4.6.	Telecommunicatie	93
4.6.1.	Inleiding	93
4.6.2.	Beïnvloeding door de elektronische snelweg	93
4.6.3.	Initiatieven tot Europese regelgeving	94
4.6.4.	Betekenis voor Nederlandse wetgeving	94

		Blz.
4.7.	Mededingingsrecht	96
4.7.1.	Inleiding	96
4.7.2.	Initiatieven op internationaal en Europees niveau	96
4.7.3.	Betekenis voor Nederlandse wetgeving	97
4.8.	Fiscaliteit	98
4.8.1.	Inleiding	98
4.8.2.	Beïnvloeding door de elektronische snelweg	98
4.8.3.	Initiatieven op internationaal niveau	98
4.8.4.	Betekenis voor de Nederlandse wetgeving	99
4.9.	Conclusies en voorstellen	100
D.	**Rechtsvergelijkende aspecten**	**101**
1.	Inleiding	101
2.	Beleidsdocumenten	101
2.1.	Europese Unie	101
2.2.	Frankrijk	102
2.3.	Duitsland	102
2.4.	Verenigd Koninkrijk	103
2.5.	Verenigde Staten	103
3.	Initiatieven tot regulering	104
3.1.	Overheidsregulering	104
3.2.	Zelfregulering	104
4.	Tot slot	105
E.	**Synthese**	**106**
Deel III	**Strategische thema's**	**109**
A.	**Inleiding**	**111**
B.	**Internationalisering en rechtsmacht**	**112**
1.	Inleiding	112
2.	Opeenstapeling van rechtsmachten	113
2.1.	Algemeen	113
2.2.	Internationale harmonisatie	113
2.3.	Vrijhavens	114
2.4.	Reikwijdte strafrechtsmacht	115
2.5.	Internationaal privaatrecht	115
3.	Handhaving van nationale wetgeving	116
3.1.	Handhaving van het strafrecht	116
3.1.1.	Internationale samenwerking	116
3.1.2.	Het vereiste van dubbele strafbaarheid	116
3.2.	Handhaving van het bestuursrecht	117
3.3.	Handhaving van het privaatrecht	117
4.	Tekort schieten van de rechtsmacht	118
5.	Nadere uitwerking van de oplossingsrichtingen	118
5.1.	Supranationale regelgeving is gewenst	118
5.2.	Internet als eigensoortig rechtsgebied	119
5.3.	Zelfregulering	120
5.4.	Oplossingen toepasbaar voor meerdere rechtsgebieden	120
6.	Conclusies en voorstellen	120
6.1.	Opeenstapeling van rechtsmachten	121
6.2.	Handhaving van nationale wetgeving	121
6.2.1.	Strafrecht	121
6.2.2.	Privaatrecht	121
6.3.	Overige onderwerpen	122
C.	**Privacy**	**123**
1.	Inleiding	123
2.	Bescherming van persoonsgegevens	124
2.1.	Vergroting van het privacybewustzijn en de zelfbescherming van de burger	125
2.2.	Het stimuleren en ondersteunen van zelfregulering op elektronische markten	126
2.3.	Het bevorderen van harmonisatie van normen en instrumenten	127
3.	Biometrische persoonsgegevens en het recht op onaantastbaarheid van het menselijk lichaam	127
4.	Anonimiteit en identiteit	129
4.1.	Anonimiteit versus identiteit	129
4.2.	Biometrie voor anonimiteit en identiteit	129
4.3.	Ondersteuning privacy door de techniek	130
5.	Vertrouwelijkheid van communicatie	130
5.1.	De vertrouwelijkheid van e-mail	130
5.2.	De strafrechtelijke bescherming van e-mail	131
6.	Conclusies en voorstellen	132
6.1.	De bescherming van persoonsgegevens	132
6.2.	Biometrie en de onaantasbaarheid van het lichaam	132
6.3.	Anonimiteit en identiteit	133
6.4.	Vertrouwelijkheid van communicatie	133
D.	**Betrouwbaarheid**	**134**
1.	Inleiding	134
2.	Technische betrouwbaarheid	134
2.1.	Beschikbaarheid van technische middelen.	134
2.2.	Bescherming tegen inbreuken door technische oorzaken	135
2.3.	Technisch onomstotelijke vastlegging van systeemgegevens over een communicatie	136
2.4.	Technische duurzaamheid van elektronische documenten	136
3.	Juridische betrouwbaarheid	137
3.1.	Transparantie van de beeldschermpresentatie	138
3.2.	Kenbaarheid van de bedoelingen van de wederpartij	139
3.3.	Bona fides, goede trouw, van de wederpartij	139
3.4.	Bevoegd handelen van de wederpartij	139
3.5.	Echtheid van documenten, berichten en transacties	140
3.6.	Identificeerbaarheid van natuurlijke personen	141
4.	TTP's	142
5.	Conclusies en voorstellen	144
5.1.	Technische betrouwbaarheid	144
5.2.	Juridische betrouwbaarheid	144
5.3.	TTP's	145
E.	**Markten**	**146**
1	Inleiding	146
2.	Mededinging en informatiemarkten	146
2.1.	Technologische turbulentie	147
2.2.	Grensoverschrijdend karakter	147
2.3.	Technische koppelingen	148
2.4.	Cross-ownerships	149
3.	Toegankelijkheid	149
3.1.	Veranderingen in de telefonie	150
3.2.	Internet	150
3.2.1.	Maatschappelijk functioneren van de burger.	151
3.2.2.	Schaarsteproblemen	151
3.2.3.	Vliegwieleffecten	151
3.2.4.	Toegankelijkheid van wetenschappelijke informatie	152
3.2.5.	Toewijzing domeinnamen	152
4.	Pluriformiteit en uitingsvormen	153
4.1.	Mediabeleid	153
4.2.	Politieke meningsvorming	154
4.3.	Culturele uitingen	155
4.4.	Schadelijke inhoud van uitingen	155
5.	Conclusies en voorstellen	156
5.1.	Mededinging	156
5.2.	Toegankelijkheid	156
5.3.	Pluriformiteit	157
F.	**Rechtshandhaving**	**158**
1.	Inleiding	158
2.	Strafrechtelijke rechtshandhaving	158
2.1.	Inleiding	158
2.2.	De effectiviteit van de handhaving: aftappen van telecommunicatie.	159
2.3.	De effectiviteit van de handhaving: bijzondere opsporingsbevoegdheden	160
2.4.	Het evenwicht met privacy	161
2.5.	Privacy enhancing technologies (PET).	161
2.6.	De markt voorop	162
2.7.	Zelfregulering	163
2.8.	Tot slot	163

		Blz.
3.	Privaatrechtelijke rechtshandhaving	163
3.1	Inleiding	163
3.2	Bewijsgaring	164
3.3.	Het in rechte geldend maken van burgerlijke rechten	165
3.3.1	Lijdelijkheid van de rechter; stelplicht en bewijslast	165
3.3.2	Het materiële bewijsrecht	165
3.3.3	Bewijsovereenkomsten	166
3.3.4	Alternatieve geschillenbeslechting	166
3.4.	Privaatrechtelijk beslag en andere maatregelen tot bewaring of tenuitvoerlegging van rechten	166
4.	Conclusies en voorstellen	168
4.1.	Algemeen	168
4.2.	Strafrechtelijke rechtshandhaving	168
4.3.	Privaatrechtelijke rechtshandhaving	169
G.	**Samenvatting en conclusies**	**170**
Deel IV	**Toetsingskader**	**173**
A.	**De legitimatie van het overheidsoptreden**	**175**
1.	Een terughoudende opstelling	175
2.	Twee hoofdtaken voor de overheid	175
3.	Een derde hoofdtaak	176
4.	Wat betekent verdringing voor de rol van de overheid?	176
B.	**Problemen van regelgeving**	**178**
C.	**Aandachtspunten voor regelgeving**	**180**
1.	Nationaal of internationaal?	180
2.	Zelfregulering of overheidsregulering?	180
3	Rechter, bestuur of wetgever?	182
3.1.	Getoetst wordt of de rechtsontwikkeling niet aan de rechter kan worden overgelaten.	182
3.2.	Getoetst wordt of overheidsoptreden langs bestuurlijke weg kan plaatsvinden.	182
3.3.	Getoetst wordt of een nadere uitwerking van het privaatrecht, met het oog op de elektronische snelweg geschikt is.	183
3.4.	Indien geen van de voorgaande opties voldoende geschikt is, wordt gekozen voor publiekrechtelijke wetgeving.	183
D.	**Het toetsingskader zelf**	**185**
Deel V	**Actiepunten**	**189**
A.	**Inleiding**	**191**
B.	**Het toetsingskader**	**192**
C.	**Implementatie van de overige voorstellen**	**193**
D.	**Actieplan**	**194**
1.	Privaatrecht	194
2.	Strafrecht (wetgeving)	195
3.	Strafrechtelijke handhaving	197
4.	Bestuursrecht	198
5.	Communicatie met de overheid	199
6.	Privacy	200
7.	Vrijheid van meningsuiting	201
8.	Biometrie en identificatie	201
9.	Trusted Third Parties	203
10.	Marktwerking	203
11.	Internationalisering en rechtsmacht (nationale uitvoering)	204
12.	internationalisering en rechtsmacht (inbreng in internationale gremia)	205
13.	Toegevoegd project: actualisering nota	207
Deel VI	**Bijlagen**	**209**

DEEL I. INLEIDEND GEDEELTE

A. ALGEMENE INLEIDING

1. Aanleiding voor de nota

Het ontstaan van de informatiesamenleving brengt de overheid een aantal belangrijke vraagstukken, die in hoge mate met elkaar samenhangen. Deze onderling verbonden kwesties leidden eerder tot het Nationaal Actieprogramma Elektronische Snelwegen (NAP). Ook bij vraagstukken op het vlak van wetgeving bleek, bijvoorbeeld bij de uitvoering van het NAP, behoefte te bestaan aan een integrale aanpak van deze vraagstukken. Die aanpak dient twee doelen:

- Vergelijkbare vraagstukken die aan de wetgever worden voorgelegd, kunnen op vergelijkbare wijze worden opgelost.
- Er kan worden bekeken in hoeverre bestaande wetgeving, die veelal is geschreven ten behoeve van de fysieke wereld, ook geschikt is in een elektronische omgeving.

Om deze redenen heeft het kabinet een visie ontwikkeld op de rol van de overheid als wetgever in de informatiesamenleving. Het kabinet verwacht dat deze visie – of in ieder geval delen daarvan – gedurende een aantal jaren stand kan houden, ondanks dat de ontwikkelingen op het gebied van de informatie- en communicatietechnologie met turbulentie gepaard gaan. Tevens worden in deze nota oplossingen aangedragen voor concrete juridische vraagstukken die zich in een elektronische omgeving voordoen.

2. Probleemstelling

Technische en maatschappelijke ontwikkelingen op het gebied van informatie en communicatie leiden tot een aantal terugkerende vragen, te weten:

- In hoeverre is overheidsoptreden in de elektronische omgeving mogelijk en zinvol?
- In welke gevallen is dit wenselijk?
- Indien tot optreden wordt besloten, welk instrumentarium moet dan worden gehanteerd?

De vragen komen voort uit een aantal lastige concrete onderwerpen op verschillende terreinen. Een paar voorbeelden: het strafrecht (denk aan kinderporno op het Internet), de telecommunicatie- en mediawetgeving (bijvoorbeeld bij de behandeling van de ontwerp-Telecommunicatiewet), het intellectuele eigendom (handhaven auteursrechten op het Internet) en het internationaal recht (welke staat heeft rechtsmacht?).
Deze nota moet ervoor zorgen dat het bevoegd gezag in staat is op een overwogen en eenduidige wijze antwoord te geven op deze vragen. Met het ontwikkelen van een visie op de rol van de overheid als wetgever, zal deze nota tevens een bijdrage leveren aan de invulling van de discussie omtrent het publiek domein, zoals bedoeld in Actielijn 3 van het NAP.
Voor het beantwoorden van deze vragen bestaan op dit moment alleen de algemene regels, zoals geformuleerd in de Aanwijzingen voor de regelgeving (zie bijlage 7). De nota beoogt deze aanwijzingen te concretiseren teneinde wetgeving te scheppen die vergelijkbare vraagstukken op vergelijkbare wijze kan oplossen.
Het ontstaan van een informatiesamenleving leidt niet alleen tot de behoefte aan een algemene visie op de rol van de wetgever, maar doet ook de vraag rijzen op welke gebieden de voor Nederland geldende regelgeving aanpassing behoeft.

3. Doel van de nota

De nota beoogt:
- Een legitimatie te geven van het overheidsoptreden tijdens de overgang naar de informatiesamenleving voor zover het instrumentarium van de wetgeving daarbij een rol kan spelen.
- Die legitimatie te concretiseren in een toetsingskader voor de wetgever.
- Op belangrijke onderdelen aan te geven wat de verschillen zijn tussen de fysieke wereld en de elektronische omgeving.
- Voorstellen te doen voor concrete vraagstukken die zich voor doen als gevolg van technologische ontwikkelingen.

Bij het realiseren van dit doel is steeds nagegaan of het bestaande juridisch instrumentarium voldoet en zo nee, of een aanpassing volstaat, of dat daarentegen geheel nieuwe normen en kaders nodig zijn. Indien een bekend sociaal verschijnsel, dat reeds bij wet is geregeld, zich onveranderd in elektronische vorm voordoet, kan een simpele aanpassing volstaan. Discriminatie in de elektronische omgeving is hiervan een evident voorbeeld. Nieuwe normen en kaders zijn daarentegen nodig indien de elektronische snelweg fundamentele veranderingen teweeg brengt, die ertoe leiden dat de bedoelingen van de wetgever moeten worden heroverwogen. Ook kunnen problemen ontstaan waarin het recht – nog – niet voorziet.

4. Opzet van de nota

De nota begint met een introductie van de begrippen, elektronische snelweg en informatiesamenleving. Deze introductie geeft op twee punten een ordening van de nota aan:
- De elektronische snelweg wordt gerangschikt in een drietal lagen, die alle drie om een ander optreden van de wetgever kunnen vragen: een netwerklaag (exploitatie van infrastructuur), een transportlaag (schakel tussen infrastructuur en gebruiker) en een inhoudslaag (toegevoegde waardediensten).
- Drie mogelijke niveaus van ontwikkeling van de informatiesamenleving worden aangegeven.

Voorts somt een begrippenlijst andere relevante begrippen op.

Deel II bevat een uitvoerige verkenning van de problematiek. Allereerst komen de belangrijkste technische vraagstukken aan de orde, die mogelijk om een reactie van de wetgever vragen. Daarna wordt de problematiek vanuit een bestuurskundige invalshoek bezien: wat betekenen ontwikkelingen in de informatiesamenleving voor interventie door de overheid? Tot slot wordt een aantal juridische verkenningen gedaan. Op welke wijze beïnvloedt de elektronische snelweg de drie traditionele rechtsgebieden, privaat-, straf- en bestuursrecht? Wat zijn de belangrijkste rechtsontwikkelingen op verschillende deelterreinen?

Uit die verkenningen zijn vijf centrale thema's gedestilleerd. Die thema's worden in deel III besproken. Het eerste thema behelst het meest fundamentele vraagstuk waarvoor de elektronische omgeving de wetgever stelt: internationalisering en rechtsmacht. De volgende drie thema's zijn inhoudelijk van aard en geven de beleidsdoelstellingen aan voor overheidsbemoeienis met de informatiesamenleving: het waarborgen van privacy, het mogelijk maken van betrouwbaar verkeer tussen burgers en het zorgdragen voor een goede werking van de informatiemarkt, waartoe burgers toegang hebben. Tot slot beschouwt het vijfde thema de handhaving van het recht. Het eerste en het laatste thema hebben betrekking op de toepassing van het recht en van de handhaving daarvan. Welke

gevolgen heeft het internationale karakter van de informatiesamenleving? Welke vragen roept de informatiesamenleving op voor de handhaving?

Deel IV van de nota geeft een gemeenschappelijk kader voor het kabinet bij vragen over wetgeving met betrekking tot de elektronische snelweg. Deel V bevat voornamelijk een opsomming van de voorstellen voor het opstellen, aanpassen of intrekken van wetgeving en voor de inbreng in internationale overlegfora.

5. Reikwijdte van de nota

Deze nota bestrijkt een breed, maar niet onbeperkt terrein. De beperkingen worden hier kort weergegeven:

- De nota heeft betrekking op de elektronische snelweg, een metafoor die staat voor het totaal aan ontwikkelingen die leiden naar de informatiesamenleving. Het gaat dus niet alleen om Internet, waarmee het begrip elektronische snelweg vaak wordt vereenzelvigd, maar tevens om allerlei andere vormen van telecommunicatie, digitale informatiedragers, elektronische betalingssystemen en dergelijke. De grote reikwijdte is gekozen om te voorkomen dat de nota slechts oplossingen aandraagt voor een deel van de vraagstukken die bij de technologische ontwikkelingen aan de dag kunnen treden. Gelet op de veranderlijkheid van de technologie en de toepassingen, zou een beperking van de nota tot Internet onvoldoende recht doen aan de problematiek. In hoofdstuk I.2 wordt hierop nader ingegaan.
- De nota beperkt zich tot die vormen van overheidsbemoeienis waar wetgeving aan de orde is of kan zijn. Dat hoeft overigens niet steeds tot het daadwerkelijk opstellen van wetgeving te leiden, zoals ook al blijkt uit de Aanwijzingen voor de regelgeving 6 en 7. Volgens die Aanwijzingen wordt onderzocht of zelfregulering niet méér geëigend is en vervolgens, indien overheidsoptreden noodzakelijk blijkt, of dat niet anders kan dan door het tot stand brengen van wetgeving. Om enig houvast te geven: de nota omvat in ieder geval de volgende overheidstaken:
  - de klassieke rechtsstatelijke waarborgtaken van de overheid, zoals de bescherming en afbakening van een aantal klassieke grondrechten (privacy, vrijheid van meningsuiting, huisrecht, briefgeheim) en het instandhouden van een aantal algemene instituties die het maatschappelijk en rechtsverkeer mogelijk maken, zoals de strafvordering, de intellectuele eigendom en het vermogensrecht;
  - toezicht op de mededinging.

6. De plaats van de nota; afstemming met andere activiteiten

Het uitbrengen van deze nota vindt plaats kort vóór de herijking van het NAP. De conclusies en voorstellen van deze nota vormen de inbreng voor het juridische gedeelte van die herijking. De implementatie van deze nota zal dan ook in het licht van deze herijking moeten worden bezien. De meer algemene voornemens van deze nota kunnen hun plaats vinden in een nieuw actieprogramma.
De nota geeft verder een aantal uitgangspunten voor wetgeving op een terrein waarop volop ontwikkelingen plaatsvinden.
Twee voor deze nota belangrijke wetsvoorstellen zijn in de Tweede Kamer in behandeling, te weten:

- Het voorstel voor een nieuwe Telecommunicatiewet[1]
- Het voorstel tot wijziging van artikel 13 van de Grondwet[2]

Deze beide wetsvoorstellen komen in deze nota aan de orde. De nota beoogt niet het wetgevingsproces van deze wetsvoorstellen, dat al vrij ver is gevorderd, te beïnvloeden.
Een derde wetsvoorstel, dat voor deze nota groot belang heeft, is het voor-

[1] IIK 25 533.
[2] IIK 25 443; aanvaard per 21 januari 1998.

stel voor een Wet bescherming persoonsgegevens. Dit voorstel zal worden ingediend min of meer gelijktijdig met het uitbrengen van deze nota. Daarnaast heeft het kabinet enkele beleidsnota's op aanpalende terreinen in voorbereiding, die nog voor de kabinetswisseling worden afgerond:

- De Minister van Justitie en de Staatssecretaris van OCW zullen aan de Tweede Kamer een nota sturen over auteursrecht en nieuwe media. De inhoud van die nota wordt afgestemd op de algemene uitgangspunten van deze nota. In de onderhavige nota wordt daarom beperkt op het auteursrecht ingegaan.
- De Minister van Economische Zaken zal een actieplan uitbrengen over elektronische handel. Het onderdeel «juridische randvoorwaarden» van dat actieplan, is overeenkomstig deze nota opgesteld.
- De Staatssecretaris van OCW zal een nota uitbrengen over het Publiek domein in de informatiesamenleving. Waar die nota ingaat op algemene taken van de overheid, heeft afstemming plaats gehad.
- De ministers van Verkeer en Waterstaat en Economische Zaken zullen een notitie uitbrengen over de eisen die worden gesteld aan «Trusted Third Parties». Deze vormen een concretisering van de voorstellen in deze nota.
- in het kader van het programma «Marktwerking, deregulering en wetgevingskwaliteit» wordt een rapport geschreven over het elektronisch verrichten van rechtshandelingen. In deze nota wordt naar dat rapport verwezen. Dit rapport zal in maart 1998 worden afgerond.

Over een aantal onderwerpen dat in deze nota aan de orde komt, vindt internationaal overleg plaats. De ontwikkelingen binnen dit overleg zijn betrokken bij de totstandkoming van deze nota.
Verder wordt melding gemaakt van een project van de Wetenschappelijke Raad voor het Regeringsbeleid over dematerialisering ten gevolge van de informatiesamenleving. Dit project overlapt gedeeltelijk met de onderhavige Kabinetsnota, maar dient een ander doel. Het schetst namelijk verwachtingen over een verder weg gelegen toekomst.

Tot slot: een belangrijk onderdeel van Actielijn 4 van het NAP is het programma «Informatietechnologie en Recht», een door een commissie van deskundigen geleid programma van wetenschappelijk onderzoek en kennisoverdracht onder verantwoordelijkheid van een interdepartementale stuurgroep. Dit programma heeft betrekking tot wetgevingsvraagstukken voortvloeiend uit de vernieuwingen in de informatietechnologie.
Het werkterrein van het programma «Informatietechnologie en Recht» vertoont een nauwe samenhang met de reikwijdte van deze nota.

7. Rechtvaardiging

Bij de totstandkoming van de nota zijn veel deskundigen betrokken, werkzaam in verschillende vakgebieden. Een structurele inbreng vanuit het bedrijfsleven had plaats via een expertisegroep, waarin personen uit verschillende sectoren van het bedrijfsleven op persoonlijke titel waren vertegenwoordigd. Ook een medewerker van de Consumentenbond maakte daarvan deel uit.
Uitgebreide contacten met de wetenschap hadden plaats in een drietal workshops die het Programmabureau Informatietechnologie en Recht had georganiseerd ter ondersteuning van de nota. Voorts hebben enkele wetenschappers als «externe dwarskijker» commentaar geleverd op eerdere versies van onderdelen van de nota.
Ter ondersteuning van de conclusies heeft een internationaal rechtsvergelijkend onderzoek plaats gehad naar de stand van de wetgeving en naar de vorming van het publieke oordeel in een aantal belangrijke Europese landen en in de Verenigde Staten. Dit onderzoek is afgerond onder verantwoordelijkheid van het Centrum voor Recht, Bestuur en Informatisering van de Katholieke Universiteit Brabant.

B. INFORMATIESAMENLEVING EN ELEKTRONISCHE SNELWEG

1. Naar de informatiesamenleving

Vanaf de jaren vijftig hebben zich grote veranderingen voltrokken in de structuur van economie en samenleving. De dienstensector is de belangrijkste bron van het nationaal inkomen geworden, belangrijker dan industrie en landbouw samen. De rol van informatie en telecommunicatie is aanzienlijk toegenomen. Een informatiesamenleving ontstaat waarin een groeiend maatschappelijk en economisch belang te beurt valt aan de informatiesector.
Onder deze informatiesector valt een scala aan bedrijven en dienstverleners: producenten van informatie- en telecommunicatietechnologie, aanbieders van telecommunicatie en postvoorzieningen, softwareproducenten, grafische bedrijven, uitgevers, producenten van amusement en cultuur, omroepen, dag- en weekbladen, persbureaus, aanbieders van multimedia, informatiediensten, bibliotheken, musea, universiteiten en hogescholen, banken en verzekeraars, accountantskantoren, advocatenfirma's, reclamebureaus, onderzoeksinstellingen, ontwerpbureaus, media-adviseurs en een scala aan andere consultants. Zij zijn allen bezig met het ontwerpen en produceren van technieken, apparaten en diensten die zich uitsluitend richten op het overbrengen van gedachten, begrippen en gevoelens.
De ontwikkeling van de informatiesamenleving zal sociale en economische veranderingen teweegbrengen. De verwachtingen over de mate van verandering lopen sterk uiteen. In de media wordt veel aandacht besteed aan mogelijke radicale maatschappelijke veranderingen. Het kabinet gaat daar voorlopig nog niet van uit. Hoewel bepaalde maatschappelijke processen en economische ontwikkelingen duidelijk invloed zullen ondervinden van de komst van elektronische media, wordt niet verwacht dat de maatschappelijke verbanden zoals wij die nu kennen zich sterk zullen wijzigen. Veranderingen die op korte termijn wel voorzienbaar zijn, zijn de volgende:

- De wereld zal nog kleiner worden. Fysieke afstand hoeft de uitwisseling van informatie, het onderhouden van sociale contacten en het aangaan van persoonlijke, culturele en economische banden niet meer in de weg te staan.
- Organisaties zullen platter worden, minder duidelijk omlijnd zijn en zich over grote gebieden uitstrekken.
- Werkzaamheden zullen minder aan plaats en tijd gebonden zijn, wat mogelijk grote gevolgen zal hebben voor de mobiliteit en het gezinsleven van werknemers.
- Van strikt nationale economieën zal nog minder sprake zijn dan nu reeds het geval is.

In de informatiesamenleving zijn bedrijven in staat veel van hun activiteiten regelmatig te verplaatsen, over de gehele wereld. Voor lokale economieën geldt derhalve dat een hoge kwaliteit van de elektronische infrastructuur, van de relevante kennisinfrastructuur en van de bijbehorende diensten een zeer belangrijk concurrentievoordeel betekent. Precies dus, zoals de kwaliteit en omvang van het wateren wegennet een belangrijke rol speelde bij de vestiging van grote industrieën.

2. De elektronische snelweg

Met elektronische snelweg wordt bedoeld: het geheel van technische infrastructuren en diensten waarmee verbindingen tot stand worden gebracht en informatie wordt bewerkt, opgeslagen en verspreid. Het is moeilijk de begrippen «elektronische snelweg» en «informatiesamenleving» precies af te bakenen. Het begrip «elektronische snelweg» is een benadering van informatie- en communicatie vanuit de techniek, de

«informatiesamenleving» verwijst naar hetzelfde fenomeen, maar beziet dit meer vanuit maatschappelijk en economisch perspectief. Deze nota zal het begrip «informatiesamenleving» gebruiken op plaatsen waar het maatschappelijke en economisch perspectief centraal staat.
De metafoor van een elektronische snelweg roept het beeld op van één naadloze informatie-infrastructuur. De praktijk is echter anders. De elektronische snelweg omvat een verscheidenheid aan technologieën, systemen, netwerken, diensten en toepassingen dat onderdeel is van, of verbonden met die «elektronische snelweg». Zo is er niet één infrastructuur, maar zijn er meer infrastructuren – het telefoonnet, Internet, protocollen, de kabel, etherfrequenties, zenderparken, GSM-netwerk, DECT-netwerk, DCS 1800-netwerk – die met elkaar verbonden zijn en de technische basis van de informatiesamenleving vormen. Op dit conglomeraat van technische structuren rust een geheel van diensten dat gebruik maakt van verschillende onderdelen en combinaties van onderdelen van de infrastructuren.

3. Technische ontwikkelingen

Internet wordt algemeen gezien als hét model voor de elektronische snelweg. Hierbij kunnen echter vraagtekens worden geplaatst. De technische ontwikkelingen houden bijvoorbeeld niet op bij de komst van Internet: moderne vormen van telecommunicatie, nieuwe technieken voor betalingen, consumentenelektronica en elektronische informatiediensten komen op ons af. De volgende technische ontwikkelingen zijn relevant:

3.1. Digitalisering

Kenmerkend voor de computertechnologie is dat zij digitaal is. Dit ligt besloten in het gebruik van de transistor. De transistor kan als een elektronische schakelaar worden toegepast, die zich in twee elektrische toestanden kan bevinden: «hoog – laag» of «aan – uit». Elektronische schakelingen die met de transistor als schakelaar worden gebouwd, kunnen wiskundig worden beschreven met tweewaardige logica, met het principe van de «uitgesloten derde». Hierdoor rekenen computers in het tweetallig, «binaire» stelsel, in plaats van het gangbare decimale, tientallige stelsel.
Transistoren komen in grote aantallen voor in de zogeheten microprocessor. De microprocessor bevat de reken- en de stuureenheid van de computer. De processor kan in de vorm van een zogenoemde chip worden geproduceerd. De chip is een stukje silicium, dat via een procédé van etsen en opdampen wordt gevormd. Een chip is opgebouwd uit een zeer groot aantal transistoren. Fabrikanten van chips slagen er in om steeds meer transistoren op een chip aan te brengen en daarmee de reken-snelheid te verhogen. Volgens de Wet van Moore verdubbelt de reken-kracht van een microprocessor in een gegeven prijsklasse iedere 18 maanden.

3.2. Miniaturisering

De elektronische componenten op de chip kunnen door verbeteringen in het fabricageproces steeds kleiner worden. De apparatuur die met deze kleinere digitale componenten wordt gebouwd, kan uiteraard ook kleiner zijn. Voorbeelden hiervan zijn de Smartcard, de GSM-telefoon, de draagbare computer en draagbare audio-apparatuur.
Er wordt tegenwoordig al gewerkt aan de ontwikkeling van een telefoon met beeldscherm, met mogelijkheden tot printen en faxen. Miniaturisering maakt dus ook de ontwikkeling van apparatuur mogelijk waarin vele functies worden geïntegreerd.

3.3. Mobiele telecommunicatie

Draadloze vormen van telecommunicatie zullen nog flink in omvang groeien. Dat is het gevolg van een aantal ontwikkelingen:

- De ingebruikname van een groot aantal communicatiesatellieten.
- Mobiele, draadloze communicatiesystemen zijn inmiddels in beginsel goedkoper dan vaste telefonieverbindingen via kabels. In ontwikkelingslanden investeert men al liever in satellietverbindingen, dan in dure, vaste verbindingen.
- Er zullen naast de telefoon- en pager-toepassingen nog draadloze PC's en dergelijke in gebruik worden genomen, zodat ook datacommunicatie door de «ether» tot de mogelijkheden gaat behoren.

Interessante ontwikkelingen vinden plaats op het gebied van de satellietcommunicatie. Satellietcommunicatie is opgekomen in de jaren 60 als de beste manier om zeer grote afstanden te overbruggen. Communicatiesatellieten werden op grote hoogte in een geostationaire baan gebracht. De opkomst van glasvezel-transmissie heeft de satelliet verdrongen en in het begin van de jaren 90 werd satelliettelefonie alleen nog gebruikt voor telecommunicatie met dunbevolkte Derde Wereld-landen en op zee. De laatste jaren begint de satellietcommunicatie echter aan een terugkeer, maar dan in een nieuwe vorm. Grote aantallen communicatiesatellieten zullen in lage, niet-geostationaire baan om de aarde worden gebracht. Het gevolg hiervan is, dat de grondstations minder nauwkeurig gericht hoeven te zijn op een enkele satelliet en daarnaast met een beperkt elektrisch vermogen kunnen werken. Mobiele satelliettelefoons komen zo binnen bereik van grote groepen gebruikers.

3.4. Opkomst van telematica

Nieuwe toepassingen bouwen verder op de mogelijkheden die telecommunicatie biedt. Dit noemt men telematica, een samentrekking van telecommunicatie en informatica. Gebaseerd op technische communicatieprotocollen worden elektronische diensten ontworpen. Bedrijven verhogen hun efficiency en effectiviteit door in de interne en externe communicatie gebruik te maken van computers, werkstations, databases, LAN's, Internet, Intranet, e-mail en mobiele telecommunicatie. De werkplek is steeds minder plaatsgebonden.

4. Ontwikkelingen in gebruik en toepassing

4.1. Convergentie van de technische middelen

De voornoemde ontwikkelingen – digitalisering, miniaturisering en de opkomst van mobiele telecommunicatie en telematica – veroorzaken verschuivingen in de vertrouwde «media». De vaste relaties tussen medium, programma en dienst vervallen. Voorbeelden van convergentie:

- Van telefoon naar telecommunicatie. Telefoonverbindingen worden allang niet meer gebruikt voor alleen maar het voeren van telefoongesprekken. Het telefoonnet wordt nu gebruikt voor beeldtelefonie, teleconferencing, datacommunicatie, telewerken en als toegangsmiddel voor e-mail en «surfen op Internet».
- Van omroepzenders naar kabelnetwerk. De omroep was aanvankelijk een publiek instituut dat bestond uit een (overzichtelijk) aantal landelijke zendgemachtigden. Met de bekabeling van Nederland namen de mogelijkheden aanzienlijk toe voor de media om de huishoudens te bereiken. Met de digitalisering van de kabel, neemt de beschikbare programmaruimte nog verder toe en wordt de kabel geschikt voor tweewegcommunicatie. De kabel wordt nu ook gebruikt voor telecommunicatie.
- Van bureaucomputer tot multimediafaciliteit. De bureaucomputer was

tot voor kort een rekenmachine en tekstverwerker, maar kan nu ook worden gebruikt als televisie, telefoon, Cd-speler, voor telewerken en Internetverbindingen.
- Van autotelefoon naar mobiele telecommunicatie. Mobiele telecommunicatie groeit sterk en blijft niet beperkt tot spraak. GSM is een volledig digitaal net, wat mogelijkheden biedt voor mobiele datacommunicatie. Het versturen van elektronische berichten en bestanden, telewerken op wisselende locaties is mogelijk met GSM.

4.2. Convergentie in het aanbod

Marktpartijen hebben belangstelling voor de nieuwe media. De telecommunicatiemarkt wordt in Europees verband geliberaliseerd. Er komt een groot aantal aanbieders van telecommunicatie, die zich bovendien niet beperken tot uitsluitend de telecommunicatie zelf. Deze partijen tonen belangstelling voor de informatievoorziening en «toegevoegde waarde-diensten». Verder bieden ook bijvoorbeeld fabrikanten van consumentenelektronica multimediadiensten.
Nieuwe machtsconcentraties ontstaan. Eén leverancier van besturingssoftware bedient het overgrote deel van de wereldmarkt en zet de facto de standaard. Op het moment dat de markt wordt geliberaliseerd, bedient de zittende aanbieder van telecommunicatie, de voormalige monopolist, de gehele nationale markt. Het koppelen van netwerken, interconnectie, tegen een redelijke prijs is essentieel voor succesvolle toetreding tot de markt. De voorwaarden voor een goede marktwerking zijn nog niet aanwezig.

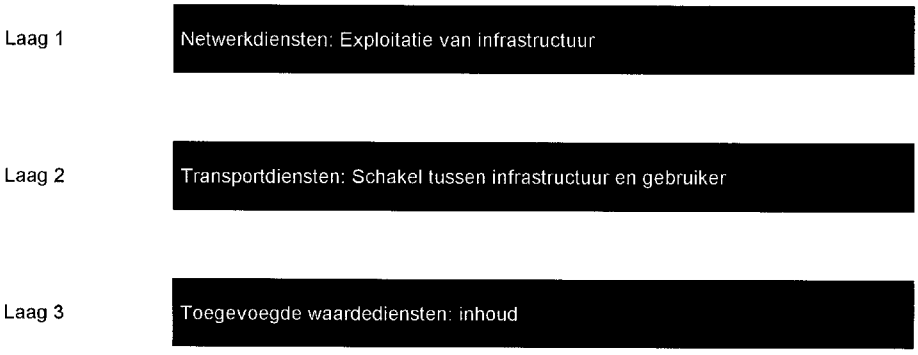
Convergentie van omroepen, telecommunicatie en computerdiensten tekent zich duidelijk af. Twee belangrijke ontwikkelingen die hierop betrekking hebben, worden zichtbaar:
- Horizontale marktdifferentiatie: van infrastructuurmonopolie in telecommunicatie, naar een oligopolie door nieuwe toetreders.
- Verticale marktintegratie: leveranciers en netwerkexploitanten richten zich op informatievoorziening, maar ook op telecommunicatiediensten.

De klassieke indeling naar medium vervaagt en wordt vervangen door een onderscheid naar activiteit.

5. Gelaagde telecommunicatiediensten

Deze ontwikkelingen leiden tot een behoefte aan een gestructureerd beeld van de «elektronische snelweg», een beeld dat bestand is tegen de stormachtige technologische veranderingen en turbulente marktontwikkelingen.
In een studie naar het toekomstige overheidsbeleid ten behoeve van de openbare elektronische informatievoorziening[1] stellen de onderzoekers dat de traditionele relatie tussen middel en dienst, zoals bijvoorbeeld kabel en televisie, telefoonnet en telefonie, in toenemende mate vervaagt. In plaats hiervan ontstaat als conceptueel model van telecommunicatie een beeld van dienstenlagen. Binnen dit model is een laag een dienst, die waarde toevoegt aan de onderliggende laag. Deze nota sluit aan bij deze gedachte en stelt de elektronische snelweg eveneens voor als een stapel van dienstenlagen:

[1] Arnbak e.a., 1990.



Deze indeling gaat niet langer uit van bestaande bedrijven en organisaties, maar van marktrollen. Een dergelijke indeling is een geschikt houvast voor de wetgever omdat niet zozeer de technische voorzieningen maar activiteiten en economische relaties centraal staan.

6. De ontwikkeling van de informatiesamenleving

Het eindpunt van de huidige onstuimige technologische en economische ontwikkelingen laat zich moeilijk voorspellen. Hoe ziet Internet er over tien jaar uit? Welke rol gaan mobiele communicatievormen spelen? Gaat elektronisch geld het chartale geld verdringen? Zal de televisie blijven, of zal deze samengaan met de computer? Zal elektronische handel van de grond komen?
Voor de lange termijn is het voor specifieke toepassingen bijna onmogelijk om goede voorspellingen te doen. De nota onderscheidt daarom drie niveaus van ontwikkeling, die niet zijn gebaseerd op inschattingen van de ontwikkelingen van specifieke toepassingen, maar op de mate waarin elektronische toepassingen doordringen in de samenleving.
Deze drie niveaus zijn «luxegoed», waarin elektronische diensten een aanvullend en een amusementskarakter hebben, «nevenschikking» waarin elektronische diensten een grote maatschappelijke en economische betekenis hebben, maar waarin geen «verdringing», de derde variant optreedt. Bij deze verdringing is het zonder toegang te hebben tot de meest voorkomende elektronische infrastructuren en diensten onmogelijk als burger te functioneren, doordat de traditionele middelen hun betekenis hebben verloren.

6.1. Luxegoed

Internet en andere elektronische diensten zijn merendeels luxegoederen, interessant voor een beperkt aantal consumenten. Hoewel een deel van de huishoudens beschikt over een modem, blijft spraaktelefonie verreweg de belangrijkste telecommunicatiedienst. Mobiele telefonie en ISDN zijn populair, maar de klassieke telefoon blijft dominant. E-mail is een informeel communicatiemiddel dat voornamelijk wordt gebruikt door particulieren en binnen bepaalde bijzondere sectoren, zoals universiteiten. Belangrijk is dat de positie van de klassieke media onaangetast blijft.

6.2. Consumptiegoed: nevenschikking

De Internet-infrastructuur bezet naast de klassieke media een belangrijke positie in het maatschappelijk verkeer. Belangrijk voor deze ontwikkeling

is de beschikbaarheid van betrouwbare publieke elektronische betaalsystemen. Een aanzienlijk deel van de huishoudens beschikt over een elektronisch postadres. Voor het zakenleven is e-mail minstens even belangrijk als het gewone briefverkeer. Naast de papieren vormen van informatie-opslag en -overdracht, nemen ook de elektronische vormen een belangrijke plaats in binnen scholen, bedrijven, universiteiten en huishoudens.

6.3. Noodzaak: verdringing

Elektronische communicatie- en betalingssystemen verdringen de oude vormen volledig. De burger kan zich niet onttrekken aan de informatiesamenleving zonder in een maatschappelijk isolement te belanden. Voorbeelden van deze verdringing zijn:
- chartaal geld door elektronisch geld
- krant door een elektronisch nieuws krant
- zakenreis door video-vergadering
- brievenpost door e-mail
- papieren documenten door digitaal-authentieke akten

De nota gaat bij haar voorstellen en voornemens uit van een niveau van nevenschikking, maar geeft, daar waar dat van belang is, ook aan wat bij een niveau van verdringing de taken van de wetgever zijn.

7. De elektronische snelweg in deze nota: kernpunten

De terminologie waarmee in documenten van overheden, media en in wetenschappelijke geschriften over de elektronische snelweg gesproken wordt wisselt sterk. «Elektronische snelweg», «informatiesamenleving», «Global Information Society», «Global Information Infrastructure» zijn termen die in wisselende betekenissen voorkomen en waarmee de lijst nog geenszins is uitgeput. In deze nota wordt de term elektronische snelweg gebruikt, in de volgende betekenis:
het geheel van technische infrastructuren en diensten waarmee verbindingen tot stand worden gebracht, informatie bewerkt wordt, informatie opgeslagen wordt en informatie verspreid wordt.
Daarnaast gebruikt de nota het begrip «informatiesamenleving», op plaatsen waar het maatschappelijk en economisch perspectief centraal staat.
Voorts wordt in deze nota een lagenmodel gebruikt, waarin onderscheiden worden een netwerk-laag (exploitatie van infrastructuur), een transportlaag (schakel tussen infrastructuur en gebruiker) en een inhoudslaag (toegevoegde waardediensten en inhoud).
Tot slot is een algemeen uitgangspunt in deze nota dat er drie verschillende niveaus van ontwikkeling van de elektronische snelweg mogelijk zijn, ieder gebaseerd op een inschatting van de mate van penetratie: «luxegoed», waarin elektronische diensten en toepassingen een aanvullend en amusementskarakter hebben, «nevenschikking», waarin elektronische diensten een grote maatschappelijke en economische betekenis hebben, maar waarin geen «verdringing», de derde variant, optreedt. Bij verdringing is het onmogelijk als burger of rechtspersoon te functioneren zonder toegang te hebben tot de meest voorkomende elektronische infrastructuren en diensten, omdat de traditionele middelen hun betekenis verloren hebben. De nota gaat veelal uit van een niveau van nevenschikking, maar besteedt ook aandacht aan de taken van de wetgever in geval van verdringing.

C. BEGRIPPENLIJST

Anonymous re-mailers.	Dienst op het Internet die E-mail doorstuurt zonder daarbij de afzender te vermelden. Op die wijze kan een anonieme e-mail worden verzonden, of kan een bijdrage aan een Usenet-groep (zie aldaar) anoniem zijn.
Anonymous server.	Dienst op het Internet waarvandaan over het Internet kan worden gesurfd zonder dat persoonsgegevens op de bezochten Internet-sites worden achtergelaten.
ASCII.	American Standard Code for Information Interchange; meestgebruikte gestandaardiseerde letterteken-set voor computers.
Bestandsrechten.	Stelsel van permissies (lees-, schrijf- en executierechten) op computerbestanden. Het computerbesturingssysteem beheert de bestandsrechten.
Biometrie.	Vaststellen van een meetbaar fysiek kenmerk, of persoonlijk kenmerk om met geautomatiseerde middelen identiteit vast te stellen.
Brute force attack.	Methode voor het kraken van een asymmetrisch versleuteld bericht door het ontbinden van een zeer groot getal in twee priemdelers.
BUPO.	(New York, december 1966). Internationaal verdrag inzake Burgerrechten en Politieke Rechten
Chip.	Sterk geminiaturiseerde (enkele vierkante millimeters) geïntegreerde schakeling van transistoren en andere onderdelen die computergeheugens en microprocessoren kunnen bevatten
Chipcard.	Pasje met chip. Een memorycard bevat alleen een geheugen(chip), een smartcard bevat ook een processor(chip) en kan dus zelf gegevens bewerken.
Content provider.	Verstrekker van informatiediensten op de elektronische snelweg.
Convergentie.	Het verschijnsel dat als gevolg van digitalisering de traditionele relatie tussen dienst en middel verdwijnt. Bijvoorbeeld: telefonie over Internet.
Cryptografie.	Geheimschrijven. Technieken voor het versleutelen en ontsleutelen van digitale opgeslagen gegevens; het versluieren van informatie.
Cryptografische sleutel.	Zeer lang (geheim) getal waarmee gegevens kunnen worden vercijferd en ontcijferd.
CSN.	Card serial number. Het serienummer van de chipcard, dat wordt afgegeven bij het betalen met een chipcard.

Cyberspace.	Oorspronkelijk een aanduiding voor een virtuele wereld, uit de cyberpunk Science Fiction (subgenre van de SF waarin computers, netwerken en hackers een belangrijke rol spelen), tegenwoordig gebruikt als synoniem met Internet en netwerken.
Datamining.	Analyse van gegevens in een database met speciale programmatuur die naar anomalieën, trends of bepaalde kenmerken zoekt.
Database.	Gestructureerde set(s) gegevens, verbonden met software om de gegevens te bewerken of terug te zoeken.
DCS1800.	Digital Cellular System, GSM-technologie voor mobiele communicatiediensten in dichtbevolkte gebieden op 1800 Mhz frequentie.
DECT.	Digital European Cordless Telecommunications. Gestandaardiseerd digitaal draadloos telefoniesysteem. Het systeem is geschikt voor PBX (Private Branch Exchange, draadloze telefoon voor bepaald bedrijf) en draadloze thuistelefoons. DECT-technologie kan een belangrijke rol gaan spelen als toegangsmiddel tot concurrerende vaste telecommunicatienetten.
Dematerialisering.	Ontwikkeling waarbij kennis en informatie belangrijke op zich zelf staande economische productiefactoren worden.
DES.	Data encryption standard; symmetrisch cryptografisch systeem.
Dienstenlagen.	Concept om telecommunicatiediensten te groeperen naar functionele kenmerken. Iedere laag heeft de onderliggende laag nodig om te kunnen functioneren en biedt diensten aan de bovengelegen laag.
Digitale technieken.	Technieken waarbij gegevensverwerking (spraak, beeld, tekst) gebeurt door rekenen met binaire getallen, die goed kunnen worden gerepresenteerd in elektrische, magnetische en optische signalen.
DMSA.	Nederlandse Associatie voor Direct marketing, Distance Selling en Sales Promotion. Gezamenlijke belangenbehartigingsorganisatie (opgericht januari 1995) van het Direct Marketing Instituut Nederland, de Nederlandse Postorderbond en het Sales Promotion Instituut Nederland.

Domeinnaam.	Voluit: Generic top-level domein. Geeft een domein op Internet aan, bijvoorbeeld Nederland (extensie .nl). Samen met de hostnaam, de naam waarmee één computer op het Internet bekend is vormt de domeinnaam de Fully Qualified Domain Name, ofwel het netwerkadres. In minjust.nl is minjust de hostcomputer van het Ministerie van Justitie en nl het domein Nederland.
EDI.	Electronic Data Interchange. Standaard voor documentenuitwisseling tussen computers van samenwerkende bedrijven. Meestgebuikte standaarden zijn variaties van ANSI X12 of EDIFACT.
EEX.	EG Verdrag betreffende de rechterlijke bevoegdheid en de erkenning en tenuitvoerlegging van beslissingen in burgerlijke en handelszaken.
EVA.	Europese Vrijhandelsassociatie.
Elektronische handel (electronic commerce).	Strikt genomen het kopen en verkopen van goederen en het overbrengen van financiële transacties via digitale netwerk-communicatie, gebruik makend van EDI (zie aldaar) en Electronic Funds Transfer (communicatiesysteem tussen betaalautomaten in winkels en banknetwerken) en workflow-controlsystemen. Inmiddels wordt het hele scala van informatie-uitwisseling tussen bedrijven onderling en tussen bedrijven en consumenten tot elektronische handel gerekend, dus ook communicatie, informatie-uitwisseling, advertenties via het WWW en Internet-activiteiten in brede zin.
Elektronische snelweg.	Het geheel van technische infrastructuren en diensten waarmee verbindingen tot stand worden gebracht, informatie bewerkt wordt, informatie opgeslagen wordt en informatie verspreid wordt.
E-mail.	Elektronische post.
Etherfrequenties.	Elektromagnetische golven die voorzien in een transmissiepad voor telecommunicatie. Frequenties vormen een schaars goed; verschillende verdelingsmechanismen kunnen worden gehanteerd; veiling en vergunning worden gehanteerd bij de verdeling van frequenties.
ETSI.	European Telecommunications Standards Institute. Europese standaardisatie-organisatie, naar analogie van de ITU-T (zie aldaar).
EVEX.	(Parallelverdrag; Verdrag van Lugano). Verdrag betreffende rechterlijke bevoegdheden en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, 1988.
EVRM.	Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (Rome, 1950).

Gegevensopslag.	Het elektronisch bewaren van gegevens zodat deze kunnen worden opgevraagd op een onbepaald tijdstip.
Gegevens-transport.	Gegevens in een telecommunicatienet.
GSM.	Global System for Mobile communications. Europese (wettelijk vastgelegde) standaard voor mobiele telecommunicatie, wordt gebruikt op de 900mhz en 1800 Mhz frequentie.
Haagse Conferentie.	(The Hague Conference on Private International Law), opgericht 1893 om de unificatie van de regels van het internationaal privaatrecht te bevorderen.
Hacken.	Onrechtmatig binnendringen in computers of netwerken.
IANA.	Internet Assigned Numbers Authority. Centraal register voor series getallentoewijzingen die bij toepassing van netwerkprotocollen van belang zijn.
ICT.	Informatie- en communicatietechnologie. Samengaan van informatietechnologie en telecommunicatietechnologie.
Interconnectie.	Bewerkstelligt de interoperabiliteit tussen openbare telecommunicatienetwerken. De klanten van verschillende netwerken kunnen (tegen betaling) gebruik maken van elkaars netwerk doordat de netwerken technisch op elkaar aansluiten.
Interface.	Technisch koppelpunt van systemen.
Internationalisering.	Ontwikkeling die het gevolg is van verbetering van communicatietechnologie en wegvallen van handelsbelemmeringen. Meer burgers en bedrijven hebben grensoverschrijdende contacten, zowel commercieel, financieel als anderszins.
Internet.	Wereldwijd computernetwerk. Fysiek verbonden door een systeem van basis-netwerken of backbone-netwerken (bijvoorbeeld: ARPAnet, NSFLNet, MILNET) waaraan transit en lokale netwerken gekoppeld zijn zoals commerciële (com), universitaire (edu) militaire (mil) en onderzoeksnetwerken (org en net). Naast de fysieke verbinding van de netwerken speelt de uitwisselbaarheid van de diverse protocollen een belangrijke rol.
Internet backbone.	Meest elementaire Infrastructuur-laag van Internet-computers en verbindingen.
Internet Relay Chat (IRC).	Medium voor real-time beeldschermconversatie via het internet.

Internet router.	Computer die Internetverkeer routeert door de Internet-backbone.
Internet Society.	Organisatie die de technische ontwikkeling van het Internet stimuleert.
Intranet.	Netwerk met Internettechnologie en Internet-achtige diensten, dat beperkt toegankelijk is (bijvoorbeeld: alleen voor één organisatie of bedrijf).
ISDN.	Integrated Services Digital Network. Set communicatiestandaarden die moeten leiden tot volledige digitalisering van het telefoonnet met extra diensten.
ISO.	International Organization for Standardization. Vrijwillige (niet op verdragen gebaseerde) standaardisatie-organisatie die onder meer computer- en communicatiestandaarden vaststelt en beheert. ISO heeft ook het OSI-lagenmodel voor telecommunicatie vastgesteld, waarvan het drielagenmodel dat in deze nota wordt gebruikt een vereenvoudiging is.
ITER.	Programma Informatietechnologie en Recht, onderdeel van het NAP (zie aldaar).
ISP.	Internet service provider, aanbieder die gebruikers toegang verleent tot Internetdiensten.
ITU-T.	Telecommunicatiestandaardisatie-afdeling van de International Telecommunications Union (voor 1 maart 1993 bekend als CCITT). ITU werkt nauw samen met alle standaardisatie-organisaties om een internationaal uniform systeem van communicatiestandaarden te scheppen.
Kabel.	Aanvankelijk bedoeld als centrale antenne inrichting. De kabel speelt nu een sleutelrol in de liberalisering van de telecommunicatiemarkt om de huishoudens toegang te bieden tot de netten van nieuwe aanbieders.
LAN.	Local Area Network. Geografisch beperkt netwerk (meestal 1 km) voor datacommunicatie, meestal in één of een aantal gebouwen.
LEO.	Low Earth Orbit. Stelsel van niet-geostationaire communicatiesatellieten voor mobiele telecommunicatie
Lex Internet.	Specifiek Internet-verdrag.
Magneetpas.	Pasje met magneetstrip. De magneetstrip heeft in vergelijking met een chipcard een zeer beperkte opslagcapaciteit en kan geen bewerkingen uitvoeren.
Mailbox.	Elektronische postbus.

Marktliberalisatie.	Het introduceren van marktwerking; de overgang van staatsmonopolie naar mededinging in telecommunicatie.
Millennium-probleem.	Het risico van falende computersystemen in het jaar 2000 ten gevolge van de vastlegging van jaartallen in geheugens en programma's in twee posities (98 in plaats van 1998). In de praktijk betekent dit dat de computer alleen de twintigste eeuw kent (2000 is dus 1900 voor de computer), waardoor programma's die met het tijdsverloop rekening houden niet de juiste datumberekening maken.
Moore, wet van.	Waargenomen wetmatigheid dat de rekenkracht van een processor in een gegeven prijsklasse, iedere 18 maanden verdubbelt.
MOT.	Meldpunt Ongebruikelijke Transacties, centraal punt waar banken ongebruikelijke (naar omvang) financiële transacties moeten aanmelden.
Multimedia.	Mens-computer interactie die text, beeld, geluid en stem omvat en veelal ook hypertext-links. De term is synoniem geworden met CD-ROM toepassingen in PC's omdat de meeste echte multimedia-toepassingen op CD-ROM staan.
NAP.	Nationaal Actieplan Elektronische Snelwegen.
Netiquette.	Beleefdheidsregels voor Usenet en mailing-lijsten. De voornaamste regels zijn: geen commerciële bijdragen, geen bijdragen die niet in de discussiegroep passen, geen persoonlijke boodschappen in nieuwsgroepen en de gewoonte om overtreders niet publiekelijk aan de schandpaal te nagelen maar via persoonlijke e-mail.
Netwerkadressen.	O.a. telefoonnummers, e-mailadressen, IP-nummers. Nummerstelsels t.b.v. gebruikers, service-contracten en technisch functioneren van telecommunicatienetten.
Netwerk-computer.	Kleine, goedkope thuiscomputer die alleen een eigen besturingssysteem heeft en een snelle verbinding met het Internet heeft. Applicatiesoftware wordt per sessie al naar gelang de behoefte van de gebruiker van het netwerk (Internet) gehaald. Volgens sommigen de opvolger van de huidige PC met eigen applicatie-software.
Netwerkprovider.	Aanbieder die een netwerk exploiteert.
NMA.	Nederlandse Mededingingsautoriteit, houdt toezicht op de naleving van de Mededingingswet.
OESO.	Organisatie voor Economische Samenwerking en Ontwikkeling.

ONP-richtlijnen.	Richtlijnen van de Europese Unie over de totstandkoming van een interne markt voor spraaktelefonie. Richtlijn 90/387/EEG is de eerste van deze serie.
Operating system.	Computerbesturingssysteem.
OPTA.	Onafhankelijke Post en Telecommunicatie Autoriteit. Houdt toezicht op de Nederlandse telecommunicatiemarkt.
Pager.	Draadloze ontvanger die signaal afgeeft als iemand de drager telefonisch wil bereiken. Moderne pagers kunnen dankzij digitale technologie alfanumerieke boodschappen ontvangen. Steeds vaker worden pagers geïntegreerd met Personal Digital Assistants (PDAs), kleine palmtop-computers die een elektronisch kladblok en uitgebreide agenda bevatten.
Paradorstrategie.	Strategie waarbij de overheid in haar eigen handelen een voorbeeld stelt, in de hoop dat dit algemeen wordt nagevolgd. Parador is een keten van Staatshotels in Spanje. Na de oorlog koos de Spaanse overheid ervoor niet in wetgeving kwaliteitscriteria voor hotels vast te leggen (teneinde daarmee het toerisme te bevorderen), maar zelf een aantal hotels te beginnen die aan hoge kwaliteitscriteria voldoen. De verwachting was dat andere hotels zich aan die criteria zouden meten. Die verwachting kwam uit.
PET.	Privacy Enhancing Technology. Alle technieken en inrichtingen die er voor zorgen de gebruikers van een netwerk geen of zo min mogelijk persoonsgegevens afgeven.
PGP.	Pretty good privacy; asymmetrisch cryptografisch systeem dat gebruikt wordt voor het versleuteld versturen van berichten.
PICS.	Platform for Internet Content Selection. Werkgroep van belanghebbenden en vertegenwoordigers van informatiebedrijven om informatie te labelen, zodat filter-software zorgt dat deze informatie niet kan worden gedownload of zichtbaar gemaakt kan worden. Oospronkelijk hulpmiddel om ouders te laten controleren of kinderen geen ongewenste informatie binnenhaalden. Tegenwoordig houdt PICS zich ook bezig met labels voor ander gebruik (o.a. auteursrecht) en geeft voorlichting over filtering software en internetproviders die zelf maatregelen nemen.
PIN.	Personal identification number, getal voor persoonsverificatie.
Prepaid card.	Anonieme SIM card die een door de operator bepaalde hoeveelheid vooruitbetaalde telefoontikken bevat.

Processor.	Central Processing Unit van een computer. Voert het centrale beheer over de andere onderdelen van de computer.
Protocol.	Een stelsel van afspraken voor het verloop van een communicatieproces. In protocollen is vastgelegd wat de standaard communicatiewijze is van een bepaald netwerk is, zowel op laag niveau (elektrische en fysieke normen, bit en byte volgorde, overdrachts- en fout-controle) als op hoog niveau (data-format, boodschapsyntaxis, dialoog van terminal naar computer).
Public key system.	Asymmetrisch cryptografisch systeem; de verzender gebruikt de openbare sleutel van de geadresseerde voor het vercijferen van het bericht, terwijl de ontvanger een bijpassende geheime sleutel hanteert voor het ontcijferen.
RFC.	Request for Comments. Serie genummerde informatiedocumenten (en soms standaarden) voor de Internet en UNIX gemeenschappen. FRC's zijn de laagste vorm van standaardisatie, de voorgestelde technische oplossingen worden vrijwillig nagevolgd en worden niet vastgelegd door een officiële standaardisatie-organisatie zoals de ANSI. Voorbeelden van RFC's: RFC 822 is het standaard format voor e-mail, RFC 1855 is een voorstel voor gedragsregels.
Scrambling.	Het volgens een complex patroon verhaspelen van gegevens zodat een derde deze niet kan interpreteren.
Service provider.	Aanbieder van telecommunicatie-diensten (elektronisch postadres, toegang tot Internet, GSM-abonnementen).
SIM kaart.	Subscriber identity module; abonneechipcard voor GSM-dienst.
Smartcard.	Pasje met processorchip, dat daardoor zelf gegevens kan bewerken.
Software.	Computerprogramma's. Systeemsoftware bestuurt de computer, applicatie-software biedt de gebruiker gespecialiseerde toepassingen, zoals tekstverwerkers, spread-sheets en spelletjes. Software is altijd georganiseerd in regels en routines (groepen regels) die instructies geven aan de computer.
Spamming.	Oorspronkelijk het plaatsen van niet relevante berichten in Usenet-nieuwsgroepen. Tegenwoordig ook een aanduiding voor het versturen van ongevraagde e-mail, meestal voor commerciële doeleinden.

Spoofing.	Oorspronkelijk de naam van een techniek om te grote belasting van netwerken te voorkomen. Veel verkeer op netwerken bestaat uit mededelingen voor netwerk-onderhoud, zoals keep-alive boodschappen. Om te zorgen dat verbindingen niet verstopt raken kan een andere dan de aangesproken computer (bijvoorbeeld een tussengelegen router) dergelijke boodschappen beantwoorden. Tegenwoordig is de term ook in gebruik voor het voor de gebruiker niet merkbaar omleiden van internetverkeer naar bijvoorbeeld een andere website of nep-website.
Standaard.	Vaste, bekendgemaakte vaststelling van technische, procedurele en/of organisatorische eigenschappen (van een apparaat, systeem of netwerk). Standaarden zijn nodig voor interoperabiliteit (samenwerking tussen systemen en netwerken), portabiliteit (gebruik van systemen of software in een nieuwe of andere omgeving) en hergebruik van systemen en apparaten. Hoe meer standaardisatie, des te meer interoperabiliteit en portabiliteit. Standaarden kunnen de facto standaarden zijn, ze worden dan wel door gebruikers en producenten algemeen erkend, maar ze zijn niet geratificeerd door een (internationale) standaardisatie-organisatie als de ETSI of de ISO.
Steganografie.	Digitale technieken voor het verbergen van informatie in grote computerbestanden.
Tappen.	Het afluisteren van (tele)communicatie.
Technologische turbulentie.	Informatietechnieken en producten volgen elkaar in hoog tempo op of convergeren tot nieuwe media. De ontwikkeling van de techniek, het maatschappelijk gebruik ervan en de sociale en juridische problemen die erdoor worden opgeroepen zijn in hoge mate
Telecommunicatie.	Iedere overdracht, uitzending of ontvangst van signalen van welke aard ook door middel van kabels, radiogolven, optische middelen of andere elektromagnetische middelen (Memorie van Toelichting nieuwe Telecommunicatiewet).
Telematica.	Samentrekking van telecommunicatie en informatica. Integratie van telecommunicatie en computertechnologie of daarop gebaseerde technieken.
Toegevoegde waardediensten.	Informatiediensten die gebruik maken van het telecommunciatienet.
Transistor.	Elektronische schakelaar; een chip bestaat uit een zeer groot aantal transistoren.

TTP.	Trusted third party; vertrouwelijke toegevoegde waardediensten. Bijvoorbeeld: elektronisch aantekenen, ontvangstbevestiging, rechtsgeldige digitale handtekening, beveiliging van elektronisch berichtenverkeer (encryptie).
UNCITRAL.	United Nations Commission on International Trade Law, VN-organisatie, opgericht 1966, met als doel te komen tot harmonisatie van handelsrecht.
UNIDROIT.	International Institute for the Unification of Private Law, opgericht 1926 als Volkenbond-organisatie, heropgericht als onafhankelijke organisatie in 1940. Doel is wegen te onderzoeken die leiden tot harmonisatie en coördinatie van privaatrecht en geleidelijk te komen tot uniforme rechtsregels.
Usenet.	(User's Network) Elektronische, veelal openbare, berichten- en discussie-areas op het Internet.
V-chip.	Geweldschip in televisietoestellen. Een toestel met een V-chip zendt geen beelden uit die (door de oproeporganisatie) voorzien zijn van een gewelds-code.
World Wide Web.	Gedeelte van het Internet voor multimedia en hypertext (snelle verbindingen tussen teksten in verschillende host-computers).
WIPO.	World Intellectual Property Organization. VN-organisatie voor industrieel eigendom (rechten op uitvindingen, merken, industriële ontwerpen en toepassingen) en auteursrecht (rechten op geschriften, muziek, kunst, beeld en geluid).
WODC.	Wetenschappelijk Onderzoeks- en Documentatie Centrum van het Ministerie van Justitie.
WTO.	Wereld Handelsorganisatie

DEEL II VERKENNINGEN

A. TECHNISCHE VERKENNING

1. Inleiding

De elektronische snelweg is in deel I-B als volgt gedefinieerd: het geheel van technische infrastructuren en diensten waarmee verbindingen tot stand worden gebracht, informatie wordt bewerkt, informatie wordt opgeslagen en informatie wordt verspreid. Dit technische karakter leidt ertoe dat in een aantal beschouwingen technische elementen centraal staan. Deze technische elementen worden in dit hoofdstuk beschreven. Het is niet de bedoeling een uitputtende beschrijving te geven van de techniek van de elektronische snelweg. De keuze om een element wél te beschrijven is gemaakt op grond van twee criteria:

- De behandeling is noodzakelijk voor een goed begrip van de elektronische snelweg.
- Het element vormt de basis voor een juridische notie.

2. Transport en opslag

Het verschil tussen de technische concepten «transport» en «opslag» is in veel wetgeving de basis voor het juridische onderscheid tussen stromende en opgeslagen informatie[1]. Opslag is ook in een digitale omgeving een goed hanteerbaar begrip. Informatie kan bijvoorbeeld op de harde schijf van een computer worden opgeslagen. Transport is daarentegen een metafoor uit de wereld van de mechanica: transport staat voor beweging, stroming en verplaatsing. In de digitale wereld is dit echter niet een technisch juiste voorstelling: transport heeft altijd een element van opslag in zich. Digitaal transport verloopt als volgt.

- Een gegevenseenheid – bit, byte en dergelijke – wordt aangeboden voor transmissie.
- Het transmissiesysteem kopieert de gegevenseenheid naar het afgelegen systeem.
- Het originele gegeven vervalt: het wordt weggegooid, overschreven of gewoon genegeerd.

Elektronisch transport van gegevens moet dus worden gezien als het op afstand kopiëren van gegevens en heeft daarmee twee elementen in zich: transmissie en opslag. Voorbeelden:

- Het maken van een afdruk van een bestand: het bestand wordt via de printerkabel gekopieerd naar het geheugen van de printer.
- Het voeren van een telefoongesprek: het spraaksignaal wordt bemonsterd en over de gegevensregisters van het digitale net gekopieerd.

In de analoge technieken kan het onderscheid transport en opslag technisch zuiver worden gemaakt. In de digitale wereld is het begrip opslag wel helder, terwijl transport een combinatie is van opslag en transmissie. Opslag als onderdeel van transport kan variëren van milliseconden tot jaren. Er is daarbij geen natuurlijk onderscheidende grens. Een dergelijk onderscheid is – technisch gezien – arbitrair.
Het juridisch gebruik van de begrippen transport en opslag moet daarom opnieuw worden bezien. Een manier om de termen nog steeds te kunnen hanteren is de volgende:

- Van opslag is sprake als gegevens kunnen worden geraadpleegd op een door de mens te bepalen tijdstip. Bijvoorbeeld: voice mail of e-mail.
- Van transport is sprake als gegevens zich in een toestand van telecommunicatie bevinden. Bijvoorbeeld: een telefoongesprek, een e-mailbericht dat zich op het Internet bevindt. Ook transportsystemen kunnen gegevens tijdelijk opslaan – wat bij digitale technologieën ook altijd gebeurt – maar, deze zijn niet te raadplegen op een door de mens te bepalen tijdstip.

[1] Zie ook aanbeveling 95 (13) van de Raad van Europa, problems with criminal procedural law connected with information technology.

Hoewel dus het verschil tussen transport en opslag in strikt technische zin moeilijk is te maken, kan de wetgever dit onderscheid wel blijven hanteren. Het onderscheidend criterium is: valt een gegeven te raadplegen op een door de mens te bepalen tijdstip?

3. Bestanden van (persoons-)gegevens

Grote gegevensbestanden, verbonden en toegankelijk via netwerken van computers, scheppen nieuwe mogelijkheden voor het zoeken naar en combineren van gegevens. Informatie die voorheen niet beschikbaar was, of informatie die verborgen bleef in de «gegevenszee» kan nu met krachtige zoekprogramma's in zeer korte tijd beschikbaar komen. Een voorbeeld: met het telefoonboek kan men bij een gegeven naam en adres een telefoonnummer vinden. Tegenwoordig bestaat er een computerprogramma dat met behulp van de telefoongids op CD-ROM de omgekeerde weg bewandelt: het vinden van naam en adres bij een gegeven telefoonnummer.
Er ontstaan nieuwe activiteiten. Datamining, «gegevens spitten», is het geautomatiseerd doorzoeken van zeer grote gegevensbestanden op specifieke kenmerken en het combineren van gegevens die verspreid in bestanden zijn opgeslagen. Een toepassing van datamining is «direct marketing». Hierbij wordt gebruik gemaakt van computerprogramma's die aankopen van consumenten analyseren en zo een profiel kunnen geven van iemands persoonlijke situatie en levensstijl. Datamining zal – als onderdeel van het thema privacy (deel IIIC) – in deze nota aan de orde komen.

4. Telecommunicatienetten

Lange tijd is er in Nederland slechts één aanbieder van spraaktelefonie geweest: PTT Telecom. Thans voltrekken zich in de telecommunicatie een aantal ingrijpende veranderingen. Aan de ene kant hebben deze plaats op het technische vlak. Daarbij gaat het met name om de vermeerdering van het aantal netwerken: GSM, DECT, ISDN. Aan de andere kant hebben deze veranderingen plaats op het vlak van de marktorganisatie: door liberalisering van de telecommunicatiemarkt zijn er straks veel meer aanbieders van telecommunicatie. Hoe de markt zich exact zal organiseren is onduidelijk, maar het is wel zeker dat er meer spelers komen. Een telecommunicatienet wordt commercieel uitgebaat door een netwerkexploitant, die zorg draagt voor de aanleg en voor het technisch onderhoud van de infrastructuur. Een netwerkexploitant verkoopt de beschikbare capaciteit. Dit kan rechtstreeks gebeuren in de vorm van abonnementen voor de eindgebruiker, of door tussenkomst van een service-provider. Een aanbieder van telecommunicatie-diensten koopt netwerkcapaciteit bij één of meer netwerkexploitanten en stelt abonnementen samen naar verschillende gebruiksprofielen. Onder andere het ontstaan van deze nieuwe netwerken leidt tot vragen voor de rechshandhaving. In deel III F komen deze vragen aan de orde.

5. Adressering en identiteit

Het bekende vaste telefoonnummer is de drager van een aantal duidelijk te onderscheiden functies: bereikbaarheid en tarifering, klantenbeheer, zoals afrekening en contractaanspraak en het beheer van het netwerk, zoals routering en aflevering, geografische locatiebepaling, bepaling van de aanbieder, technisch onderhoud van de aansluiting. Hierdoor is dit telefoonnummer – op de elektronische snelweg is dit het netwerkadres – een geschikt juridisch aangrijpingspunt. In moderne telecommunicatienetten hebben nummers echter niet al deze functies. Niettemin blijft een

nummer, of een netwerkadres, in belangrijke mate verbonden met de gebruiker. Het is echter niet een erg betrouwbaar gegeven.
Een betrouwbare vaststelling van een persoons-identiteit op de elektronische snelweg is essentieel voor het tot stand komen van elektronische handel. Identificatie kan – afhankelijk van de toepassing – gebeuren op verschillende niveaus van sterkte. Identificatie in de hoogste graad betekent het afstaan van een uniek en onvervreemdbaar persoonskenmerk. Betrouwbare biometrische technieken zijn inmiddels beschikbaar gekomen, maar grootschalige toepassingen kunnen pas worden verwacht na internationale processen van technische standaardisatie. De komende jaren zal er naar verwachting nog vooral sprake zijn van zwakkere vormen van elektronische persoons-identificatie. Een bekende vorm is het «personal identification number», de PIN-code. De PIN is, in tegenstelling tot wat de afkorting suggereert, persoonlijk noch identificerend. De PIN is een vervreemdbaar kenmerk – men kan het afstaan aan een derde – en evenmin uniek: met vier cijfers kunnen in principe 10 000 getallen gevormd worden; een PIN wordt dus door vele honderden gebruikers gedeeld. Het belang van adressen en identiteit voor de ontwikkeling van de elektronische snelweg vergt nadere aandacht van de overheid[1].

6. Open en besloten communicatie

Van open communicatie is sprake, wanneer het signaal een distributief karakter heeft. Duidelijke voorbeelden van open communicatievormen zijn radio en televisie. Er is sprake van besloten communicatie als een signaal gericht of geadresseerd is. Besloten communicatie kan worden geleverd door een openbaar netwerk. Openbaar in de zin van: een publiek toegankelijke dienst, zoals de openbare telefonie.
In een aantal gevallen kan het open of besloten karakter van communicatie niet aan de hand van technische criteria worden vastgesteld. Een voorbeeld hiervan vormt spamming, een techniek van het verspreiden van reclameboodschappen door middel van e-mail. Spam is weliswaar geadresseerde e-mail, maar gezien de schaal van verspreiding is het zeer de vraag of dit moet worden aangemerkt als een besloten vorm van communicatie.
Bij open vormen van communicatie is geen sprake van een bijzonder verband tussen de deelnemers. De deelnemers kunnen vrij toetreden. Voorbeelden van open communicatievormen zijn radio- en televisie-uitzendingen en Internet-discussiegroepen. Het onderscheid tussen open en besloten communicatie wordt dus niet door de techniek bepaald, het is een maatschappelijk onderscheid.
Voor de wetgever betekent dit, dat niet automatisch uit de gebruikte techniek blijkt van welke communicatievorm sprake is. Waar dit onderscheid van belang is zal de wetgever dit uitdrukkelijk moeten aangegeven.

7. Digitaal-elektronische betrouwbaarheid

Op de elektronische snelweg vinden het verkeer en de opslag van gegevens plaats door tussenkomst van technische middelen. Veel handelingen die vroeger niet zonder de tussenkomst van een persoon tot stand konden komen, worden nu geheel automatisch afgehandeld. Men kan hierbij denken aan geld halen bij een bank: vroeger kwam daar altijd een klerk bij kijken, nu gebeurt alles automatisch. Meer en meer wordt het maatschappelijk en economisch verkeer afhankelijk van de goede werking van apparatuur. De betrouwbaarheid van dergelijke apparatuur is dus van groot belang. Aan de betrouwbaarheid van de elektronische snelweg en de rol die de overheid daarin kan spelen, is Deel III-D gewijd. Hier gaat het om een aantal technische aspecten van betrouwbaarheid.

[1] Zie daarvoor: deel III, C.4, D.3 en E.3.

7.1. Het kernprobleem: de verhouding tussen kopie en origineel

Er is een kernprobleem dat niet met technische ingrepen kan worden opgelost en dat een gevolg is van het digitale karakter van de elektronische snelweg: de verhouding tussen origineel en kopie. Digitalisering van gegevens en processen heeft tot gevolg dat de oorspronkelijke drager van digitale gegevens geen sporen nalaat in het signaal. De geluidskwaliteit van een digitale muziekopname bijvoorbeeld, is niet afhankelijk van de drager, een CD.
Dat digitale gegevens zonder kwaliteitsverlies kunnen worden gekopieerd is hiervan ook een gevolg. Dit is een principieel verschil met het kopiëren van analoge gegevensdragers. De analoge drager laat altijd sporen na in het signaal. De analoge gegevensdrager verstoort het origineel: een kopie op een muziekcassette voegt ruis toe. Waar de gegevensdrager van het origineel met analoge opslagtechnieken altijd «vingerafdrukken» achterlaat op de kopie, laat de digitale gegevensdrager geen sporen na. Digitale gegevens staan geheel los van de materiële gegevensdrager en zijn perfect en onbeperkt kopieerbaar: er is dus geen verschil tussen kopie en origineel. Dit maakt onder andere dat eigendom van informatie geen goed hanteerbaar juridisch begrip is.

7.2. Beschikbaarheid van technische middelen

Gegevens zijn niet meer los te gebruiken van hun opslag en transmissietechnieken. Dat maakt de elektronische snelweg kwetsbaar:
- Kwetsbaarheid voor inbreuken door technische oorzaken. De kwaliteit van de techniek bepaalt de verwachte levensduur. De gevolgen van falende techniek kunnen worden ondervangen door replicatie van de kritische delen van systemen en netten. Moderne telefooncentrales en computersystemen in kritische toepassingen zijn dubbel, drievoudig of zelfs viervoudig uitgevoerd.
- Een tekort aan technische middelen om aan de vraag te kunnen voldoen: congestietoon, of geen kiestoon bij de telefoon, de trage binnenkomst van gegevens van Internet, de langzame, of onmogelijke aflevering van een e-mail.
- De duurzaamheid van het medium. Een document zal misschien na 20 jaar nog leesbaar moeten zijn. Dit betekent dat de gegevensdrager ook zo lang mee moet gaan. Het computersysteem dat de gegevens kan verwerken, moet dan nog beschikbaar zijn. De digitale code waarin de informatie is bewaard, moet nog interpreteerbaar zijn. Gezien de snelheid waarmee de informatie- en communicatietechnologieën elkaar opvolgen, zijn deze eisen allerminst vanzelfsprekend.

Betrouwbaarheid van communicatie is een economisch vraagstuk. Door middel van investeringen en onderhoud kan het niveau van betrouwbaarheid – in de zin van beschikbaarheid van middelen – worden gekozen.

7.3. Presentatiekwaliteit

Het gaat hierbij om de nauwkeurigheid en integriteit van de informatie, zoals die de ontvanger bereikt. De afzender wil dat de informatie de ontvanger onvervormd bereikt. De ontvanger wil een natuurgetrouwe weergave van het origineel. Een voorbeeld: partij A biedt informatie aan bij computersysteem B. Computers kunnen uitsluitend digitale gegevens verwerken en daarom zal de informatie moeten worden gedigitaliseerd. Omgekeerd zal computersysteem C de gegevens moeten decoderen en de informatie moeten presenteren aan partij D. De nauwkeurigheid waarmee deze omzettingen plaats vinden zijn bepalend voor de kwaliteit van de informatieoverdracht en daarmee voor de verstaanbaarheid van spraak, de herkenbaarheid van beeld, of de leesbaarheid van tekst.

7.4. Autorisatie, rechtenbeheer en vertrouwelijkheid

Gebruikers en groepen gebruikers willen informatie voor zichzelf houden en willen zelf kunnen bepalen wie van informatie kennis kan nemen. In beginsel gaat het om de volgende rechten op informatie uit digitale gegevens:

- Leesrechten: de bevoegdheid om kennis te nemen van informatie.
- Schrijfrechten: de bevoegdheid om informatie te veranderen of toe te voegen.
- Executierechten: de bevoegdheid om een programma te gebruiken.

Autorisatieprocedures moeten aangeven wie welke rechten heeft. Immers, de vertrouwelijkheid van besloten communicatie komt in gevaar wanneer een autorisatieprocedure iemand toegang geeft die geen toegangsrecht heeft, of iemand een verkeerd recht toewijst. Het handhaven van de betrouwbaarheid door rechtenbeheer en autorisatie zal in technisch complexe omgevingen voornamelijk aan de techniek worden overgelaten. Leesrechten kunnen worden gehandhaafd door middel van cryptografie: een versleuteld bestand kan niet worden gelezen (zie voor een verdere beschrijving van cryptografie hierna onder 7.5).
Een schrijfzegel kan zorg dragen voor het opsporen van inbreuken op de integriteit van gegevens. Een schrijfzegel speelt dus bij de schrijfrechten een belangrijke rol. Een schrijfzegel is een zegel in de klassieke betekenis: een verbroken zegel is eenvoudig te herkennen. Maar het zegel kan ook vervalst zijn. De gegevens zijn dan veranderd en er is een nieuw passend zegel aangemaakt. Om vervalsingen van bestanden tegen te gaan, moet weer worden vertrouwd op de kwaliteit van het computerbesturingssysteem. Vervalsingen in een telecommunicatie-omgeving kunnen ook voorkomen, het zogeheten «spoofing». De kwaliteit van de toegepaste technische en menselijke communicatieprotocollen bepalen de betrouwbaarheid van de communicatie.
Een executiezegel dient illegaal gebruik van software te voorkomen. Het computerbesturingssysteem kan ook hierin een rol spelen. Een andere oplossing ligt in de combinatie van speciale software en hardware. Zo wordt bij een softwarepakket soms een speciale steker geleverd die op een seriële poort van de PC kan worden geplaatst. Het programma werkt alleen met de steker, die beperkt bij de software wordt meegeleverd. Alleen de koper van het originele pakket kan de software gebruiken.
Omdat de digitale techniek zo nauw betrokken is bij de beveiliging en vertrouwelijkheid van gegevens – bijvoorbeeld digitale akten, digitaal verwerkte medische gegevens – en juist omdat de techniek zo complex is, kan niet van iedere burger voldoende inzicht worden verwacht in de effectiviteit van de technieken. Dit kan reden zijn voor technologie-afhankelijke regelgeving.

7.5. Cryptografie

Cryptografische technieken spelen een belangrijke rol bij verschillende vormen van betrouwbaarheid. Cryptografie is geheimschrift. Informatie wordt digitaal weergegeven en vervolgens vercijferd met behulp van een digitaal codewoord, een getal. De vercijferde gegevens worden verstuurd of opgeslagen. De ontvanger kan de informatie reconstrueren met behulp van de ontcijfersleutel.
Er zijn twee basisvormen voor cryptografische systemen: de symmetrische en de asymmetrische. In een symmetrisch cryptografisch systeem is de ontcijfersleutel gelijk aan het codewoord waarmee het bericht is vercijferd. Een symmetrisch systeem kan dus alleen maar worden gebruikt als de deelnemende partijen eerst de sleutels uitwisselen. Symmetrische sleutelsystemen zijn zeer geschikt voor besloten organisaties die tevoren afspraken kunnen maken over hun interne

communicatiegeheimen, bijvoorbeeld bij de strijdkrachten. Maar ook: criminele organisaties. DES, de «data encryption standaard», is een voorbeeld van een symmetrisch sleutelsysteem.
In de regel geldt dat de encryptietechniek open is – dat wil zeggen: de procedure is openbaar – en de sleutel is geheim. De veiligheid ligt dus in het bewaren van het geheim. Het doorbreken van het geheim moet gebeuren door systematisch proberen van alle sleutels, door middel van de zogeheten «exhaustive search»[1].
In een asymmetrisch, «public key», cryptografisch systeem zijn de vercijfer- en ontcijfersleutel verschillend. Eén sleutel blijft geheim (G), de andere wordt openbaar gemaakt (O). Voor een geheime boodschap aan een persoon wordt diens openbare sleutel O opgevraagd, bijvoorbeeld op het Internet. De boodschap wordt vercijferd met sleutel O en verstuurd. Alleen de betreffende persoon kan met de geheime sleutel G het bericht weer leesbaar maken. De openbare sleutel is het product van twee zeer grote priemgetallen. De geheime sleutel is de factorisatie van de openbare sleutel (de priemgetallen).
Het aantrekkelijke van asymmetrische cryptografie is dat partijen kunnen communiceren zonder tevoren bij elkaar te komen voor het uitwisselen van sleutels. Onbekenden kunnen vertrouwelijk communiceren. Een interessante toepassing van asymmetrische cryptografie is het authenticeren van een boodschap: de zender vercijfert de boodschap eerst met zijn geheime sleutel G en vervolgens nogmaals met de openbare sleutel van de ontvanger. De ontvanger ontcijfert het bericht eerst met de eigen geheime sleutel. Het resultaat wordt nogmaals ontcijferd met de openbare sleutel van de zender. Als de tweede ontcijfering «klare tekst» oplevert is aangetoond waar het bericht vandaan kwam.
Het breken van de code waarin een bericht is verzonden, gebeurt door het zoeken naar de factorisatie van de openbare sleutel. Het ontbinden in factoren van een groot getal is een uitputtende rekenklus en hierin ligt de veiligheid van een asymmetrisch cryptografisch systeem. Het breken van het sleutelgeheim van een vercijferd bericht – de zogeheten «brute force attack», BFA – is een ongelijke wapenwedloop in computer-rekenkracht. Een voorbeeld[2]: de encryptiesleutel van 40 bits wordt verdubbeld. De gebruiker heeft nu een ongeveer 6 maal krachtiger computer nodig om een bericht even snel te ontcijferen als voorheen. Echter, voor een BFA is nu 1000 miljard (2^{40}) meer rekenkracht nodig.
Het voorgaande neemt niet weg dat de voortschrijdende technologie mogelijkheden kan gaan bieden, die het doorbreken van versleuteling ook in de toekomst mogelijk en wellicht zelfs eenvoudiger maken.

7.6. Betrouwbare elektronische betaal- en geldsystemen

In de informatiesamenleving zal een grote behoefte bestaan aan betrouwbaar elektronisch geld om via netwerken transacties af te sluiten. Hoewel het moderne girale geldverkeer door de komst van gelduitgifte-automaten, PIN-betalingen, credit-cards en telebankieren inmiddels sterk afhankelijk is geworden van elektronica en techniek, verschilt elektronisch geld wezenlijk van modern giraal geldverkeer.
Elektronisch geavanceerd giraal verkeer houdt in wezen niets anders in dan een snelle administrering van mutaties van tegoeden. Het elektronische signaal, bijvoorbeeld tussen een gelduitgifte-automaat en een interbancair-netwerk, vertegenwoordigt op zichzelf geen waarde, maar kan alleen waarde ontsluiten als aan andere voorwaarden wordt voldaan, zoals het gelijktijdig verzenden van een autorisatie-signaal. Bij elektronisch geld vertegenwoordigt het signaal zelf een waarde. Bij een betrouwbaar elektronisch betaal- en geldsysteem kan een dergelijk waardevol signaal niet worden gekopieerd of ongeautoriseerd worden verzonden. De huidige interernet-betalingen – I-Pay – zijn juridisch niet meer of minder dan een vorm van «gewone» girale betaling[3]. Ook

[1] DES hanteert een sleutellengte van 56 bits. Het aantal sleutels dat hiermee kan worden gegenereerd is zo groot dat een exhaustive search – ook door een supercomputer – geen reële optie meer is.
[2] Craats, J. van de, 1991.
[3] Mr R.E. van Esch en mr dr R.E. de Rooy, Juridische aspecten van Internetbetalingen, Nederlands Juristenblad (speciaal Recht op de elektronische snelweg), 15 november 1996.

chipknip/chipperbetalingen hangen direct samen met de gegevens van de bij een betalingshandeling betrokken rekeninghouders/chipkaarthouders. Vanuit de klant en de winkelier gezien lijken deze betalingen anoniem, maar het spoor (audit-trail) wordt steeds vastgelegd, zodat herkomst en bestemming steeds zijn na te gaan. Van (anonieme) niet op personen herleidbare betalingen of van geld aan toonder is, tenminste vanuit de bank of de rechtshandhavende overheid gezien, geen sprake.
Op dit moment zijn twee vormen van elektronisch geld in ontwikkeling: de chipcard en elektronische betalingen via Internet. Een betaling met een chipcard verloopt als volgt. Een rekeninghouder zet een bedrag op zijn chipcard bij een kaartoplader, bij de bank, thuis met een modem, of in een telefooncel. Voorlopig zal een pincode worden gebruikt voor de verificatie bij het opwaarderen van de kaart. Het bedrag wordt van de rekening van de kaarthouder op een centrale rekening gestort. Op de chipcard van de gebruiker wordt slechts het tegoed geadministreerd. Bij een betaling met de chipcard wordt de kaart in een kaartlezer geplaatst, een eenvoudige hostcomputer die de chip op de chipcard activeert. Als de echtheid van de kaart is vastgesteld, wordt het bedrag afgeboekt in het geheugen van de chipcard en bijgeschreven in het geheugen van de hostcomputer.
Chipcards geven de gebruikers een betere positie tegenover de bank dan bij betalingen met PIN of met een creditcard het geval is. Indien de bank de uitgifte van kaarten goed regisseert, is vervalsing van kaarten vooralsnog niet aan de orde. De chipcard verschilt van de magnetische betaalpas in de wijze waarop kritische gegevens zijn beveiligd. Bij de huidige magnetische betaalpas zijn de geheime gegevens «open en bloot» opgeslagen op de magneetstrip. Met behulp van een kaartlezer en een eenvoudige PC kunnen deze gegevens worden gekopieerd en de PIN-code achterhaald, waarna de kaart kan worden gebruikt. Bij een chipcard zijn alle data afgeschermd.
Een betaling via Internet kan er als volgt uitzien. Een koper op Internet opent het transactieprotocol door een bericht aan een aanbieder van een product of dienst te zenden. De aanbieder antwoordt met een elektronische rekening, waarop de koper het bericht van betaling verstuurt. Vervolgens begint de computer van de verkoper, eveneens via het Internet, een autorisatieprocedure bij de computer van zijn bank. Deze bankcomputer wikkelt de boeking af over het besloten bancaire communicatienetwerk en besluit de transactie met het versturen van een bevestigingsbericht naar de computer van de koper. Bij de ontwikkeling en beoordeling van elektronisch geld zijn de technische en juridische betrouwbaarheid (zie deel III D) van groot belang.
Het is onzeker of, wanneer en op welke schaal elektronisch geld door bedrijven en particulieren gebruikt gaat worden. Technisch is betrouwbaar elektronisch geld mogelijk, maar dat is niet de enige factor die bepaalt of en wanneer elektronisch geld maatschappelijk wordt aanvaard. Schattingen van deskundigen lopen uiteen van 10 tot meer dan 20 jaar. Ook is onduidelijk hoe elektronisch geld kan inburgeren als wettig betaalmiddel. Dit hangt niet alleen van de wetgever af, omdat de status van wettig betaalmiddel ook door jurisprudentie tot stand kan komen. Daarnaast verschillen deskundigen van mening over de behoefte aan elektronisch geld. Met name in landen waarin elektronisch betalingsverkeer met chipcards (girale betalingsprocedures zoals pinpas-, chipper- en chipknip-betalingen) een hoge vlucht lijkt te nemen, is er waarschijnlijk minder behoefte aan elektronisch geld in strikte zin. Internationaal heeft de elektronische creditcard-transactie – hoewel duur en fraudegevoelig – waarschijnlijk meer kansen dan elektronisch geld in strikte zin, omdat de consument er al op grote schaal mee vertrouwd is geraakt.

8. Conclusies en voorstellen

- Een onderscheid tussen kopie en origineel is bij digitaal opgeslagen informatie niet te maken. Eigendom van informatie is hierdoor geen goed hanteerbaar juridisch begrip. Het juridische onderscheid tussen transport en opslag kan in wetgeving gehanteerd blijven worden, mits als onderscheidend criterium wordt genomen: kunnen gegevens op een door de mens te bepalen tijdstip worden geraadpleegd?
- Het onderscheid tussen open en besloten communicatie ligt niet besloten in het verschil tussen publieke en private middelen, noch blijkt dit onderscheid uit de techniek: het is een maatschappelijk onderscheid, dat wordt gemaakt door de gebruiker van deze middelen. Waar dit onderscheid van belang is zal de wetgever uitdrukkelijk moeten aangeven welke handelingen hij open acht, en welke besloten.
- Omdat de digitale techniek zo nauw betrokken is bij de beveiliging en vertrouwelijkheid van gegevens – bijvoorbeeld digitale akten, digitaal verwerkte medische gegevens – en juist omdat de techniek zo complex is, kan niet van iedere burger voldoende inzicht worden verwacht in de effectiviteit van de technieken. Dit kan reden zijn voor meer technologie-afhankelijke regelgeving.

B. BESTUURSKUNDIGE VERKENNING

1. Inleiding

Wat betekent de verdere ontwikkeling van de informatiesamenleving voor de rol en positie van de overheid in het algemeen? Wat mag er van haar worden verwacht en welke mogelijkheden heeft zij om die verwachtingen waar te maken? Wat de overheid moet doen in de informatiesamenleving, hoe zij haar sturingsfunctie dient op te vatten en welke overwegingen bij deze keuze betrokken worden, is op vele plaatsen onderwerp van reflectie. De voornaamste visies zullen in deze analyse aan bod komen en beoordeeld worden. Een afgewogen keuze kan alleen worden gemaakt op grond van een compleet beeld van de informatiesamenleving. Daarom zullen allereerst de voornaamste elementen van de informatiesamenleving worden geschetst.

2. De informatiesamenleving

In de inleiding is reeds geschetst dat ons land zich in de overgang bevindt naar een informatiesamenleving. Hoe die informatiesamenleving er uit zal zien, valt nu nog niet te zeggen. In de inleiding zijn daarom drie mogelijke niveaus van geschetst, die ieder tot andere maatschappelijke verschuivingen zullen leiden. Het gaat om de niveaus: luxe goed, nevenschikking en verdringing. De nota gaat uit van nevenschikking, maar geeft ook aan wat de taken van de wetgever moeten zijn in het geval van verdringing. Voor zover nu valt na te gaan, zijn drie aspecten van bijzonder belang voor een nadere plaatsbepaling van de rol van de overheid in de informatiesamenleving. Die aspecten zijn:

- *Dematerialisering:* kennis, diensten en informatie die niet in een tastbare vorm zijn neergelegd vormen de motor van de economie. Bij digitale vastlegging is informatie niet meer gebonden aan een bepaalde fysieke drager of plaats. Digitaal vastgelegde informatie is voorts onuitputtelijk, want zij kan oneindig worden gekopieerd, zonder dat dit leidt tot kwaliteitsverlies of vernietiging.
- *Internationalisering:* De informatiesamenleving is vooral een open samenleving. Informatie is nauwelijks aan plaats en staat gebonden en kan zeer snel doordringen in vele hoeken van de samenleving. Economisch en sociale ontwikkelingen zullen nog meer dan in het verleden hun oorsprong vinden in bronnen die buiten het bereik van de nationale overheid liggen.
- *Technologische turbulentie:* Nieuwe informatietechnieken en producten volgen elkaar in hoog tempo op, of convergeren tot nieuwe media. De ontwikkeling van de techniek, het maatschappelijk gebruik ervan en de sociale en juridische problemen die erdoor worden opgeroepen, zijn in hoge mate onvoorspelbaar en kennen een hoge omloopsnelheid.

Deze fundamentele kenmerken van de informatiesamenleving hebben zowel gevolg voor de legitimatie van het overheidsoptreden, als voor de instrumentatie van het overheidsoptreden.

3. De overheid

Voor een beter begrip van de rol van de overheid in de informatiesamenleving is het nuttig terug te blikken op die rol in de industriële samenleving. Naar analogie van Geelhoed kan men vier belangrijke functies van de overheid onderscheiden[1]:

1. *De ordenende functie:* De overheid stelt normen en procedures vast voor een ordelijk verloop van het maatschappelijk verkeer.
2. *De presterende functie:* De overheid neemt zelf de productie van een

[1] Geelhoed, L.A., 1996.

aantal publieke goederen, zoals infrastructuur, nutsvoorzieningen, onderwijs en openbare voorzieningen, ter hand.
3. *Verzorgende functie:* De overheid zorgt voor een stelsel van sociale zekerheid en sociale voorzieningen.
4. *Sturende functie:* De overheid grijpt direct in maatschappelijke ontwikkelingen, waarbij de overheid zelf uitvoering geeft aan de interventie, bijvoorbeeld bij de ruimtelijke ordening.

In de loop van deze eeuw heeft de overheid al deze functies ter hand genomen. Vanaf het einde van de jaren '70 wordt het overheidsoptreden door diverse partijen echter steeds kritischer bezien. De oliecrisis en de daarop volgende economische recessie creëerden een zeer directe noodzaak om in de overheidsuitgaven te snijden. Het wordt duidelijk dat de overheid haar ambities moet beperken. Maar niet alleen fiscaal conservatieve economen en politici leveren kritiek op de overheid en haar ruime taken en ambities. Onderzoekers wijzen er herhaaldelijk op dat de interveniërende overheid niet succesvol optreedt. De overheid die in de jaren vijftig en zestig, ten tijde van de uitbouw van de verzorgingsstaat nog als oplosser van problemen werd gezien, wordt nu steeds meer gezien als de veroorzaker daarvan. De late jaren '70 en de jaren '80 staan dan ook in het teken van forse veranderingen bij de overheid. Zowel het apparaat als de ambities worden onder handen genomen. Hoewel niet al deze operaties in het gewenste tempo en met het gewenste succes worden uitgevoerd[1] leiden ze in ieder geval tot een belangrijke mentaliteitsverandering. De overheid is niet meer de partij die vanzelfsprekend handelt en reguleert. Ook andere partijen wordt gevraagd zich te buigen over maatschappelijke vraagstukken.
De overheid exploreert actief nieuwe sturingsmogelijkheden «op afstand». Men kan hierbij denken aan wat De Vroom «associatieve zelfregulering»[2] noemt: georganiseerde belangengroepen ... (die) zelf deelnemen aan de opstelling of uitvoering van regels en normen die het eigen gedrag moeten sturen, zoals bijvoorbeeld de BOVAG[3]. Andere sturingsvormen die een minder actieve rol van de centrale overheid vergen zijn decentralisatie, waarbij overheden op lager niveau een grotere rol moeten gaan spelen, deregulering, waarbij de overheid het aantal regels vermindert en privatisering. In deze periode worden ze actief gepropageerd en getoetst.
Een andere belangrijke verandering in deze periode is de groei van regelgeving vanuit de Europese Unie. Steeds vaker moet de Nederlandse overheid in haar ambities overeenstemming zien te vinden binnen de Europese Unie. Dit geldt zeker nu de Europese Unie steeds meer beleidsterreinen gaat omvatten.
Al deze ontwikkelingen hebben de rol van de overheid en met name de relatie van de overheid tot de markt, centraal op de politieke agenda gezet. Het kabinet erkent expliciet dat de overheid niet altijd een hoofdrol kan spelen bij maatschappelijke processen. Zoals het in het regeerakkoord[4] staat: «Burgers nemen de overheid de maat van haar eigen voornemens en constateren steeds vaker dat het resultaat tekort schiet. Zo blijven problemen liggen en wordt de politiek ongeloofwaardig».
Het huidige kabinet heeft gekozen voor twee duidelijke lijnen:
- *Bestuurlijke vernieuwing.* Gericht op het verminderen van bestuurlijke sclerose, onder andere door:
  - meer samenhang in het beleid
  - departementen zich met kerntaken bezig te laten bezig houden, waardoor ze kleiner en slagvaardiger worden
  - de oprichting van een bestuursdienst
- *Dynamiek.* Gericht op het flexibeler maken van de economie, onder andere door:
  - minder regelgeving en minder administratieve druk voor bedrijven en individuen
  - vermindering van het aantal concurrentiebeperkende maatregelen

[1] Derksen, W., 1989.
[2] Vroom, B. de, 1989.
[3] Witteveen, W.J., 1989.
[4] Kabinet-Kok, 1994, p. 59.

– stappen ter facilitatie van een 24-uurs economie
– betere en beter toegankelijke kennisinfrastructuur
– programma marktwerking, deregulering en wetgevingskwaliteit

In termen van de functies van Geelhoed komt de ontwikkeling neer op een sterke afname van de presterende functie, een beperking van de verzorgende functie en een verschuiving van de sturende functie naar de ordenende functie. Ordening komt vanaf het einde van de jaren '70 in de overheidsactiviteiten steeds centraler te staan.

4. Visies op de overheid in de informatiesamenleving

Samenleving en overheid ondergaan dus belangrijke veranderingen. De vraag is nu, wat deze veranderingen betekenen voor het perspectief van de overheid in de informatiesamenleving. Vormt de informatiesamenleving een geheel nieuw probleem, dat een fundamentele verandering van de rol van de overheid vereist? Of is er eerder sprake van continuïteit?
De rol van de overheid in de informatiesamenleving heeft veel aandacht gekregen, zowel in de internationale bestuurskundige en economische literatuur, als in een reeks van beleidsdocumenten van internationale organisaties en regeringen. De waardering van de mogelijkheden voor de overheid om op te treden, lopen sterk uiteen. In grote lijnen kan men drie verschillende standpunten in de discussie en beleidsstukken onderscheiden.

4.1. De onmachtige overheid

Het centrale thema van veel, met name academische visies op de toekomstige, postmoderne overheid is onmacht. De sturende positie die de natiestaat heeft verworven, wordt afgebroken. Hiervoor worden de volgende oorzaken genoemd:

1. *De informatiesamenleving zal meer transparantie kennen.* De kern van deze stelling is dat informatie oorzaak van macht kan zijn, bijvoorbeeld doordat sommige beslissingen alleen op grond van bepaalde informatie kunnen worden genomen, of – misschien wel belangrijker – gerechtvaardigd kunnen worden. De verhoogde transparantie van de informatiesamenleving – informatie wordt sneller en over meer mensen verspreid – leidt ertoe, dat de overheid haar unieke informatiepositie moet afstaan, of in ieder geval moet delen met andere partijen. Dit kunnen de media zijn, maar ook grote bedrijven die door investeringen in hun informatie-infrastructuur een bepaalde informatiepositie verwerven.
2. *Turbulentie.* Veranderingen zullen zich in sneller tempo voltrekken. Dat informatie sneller in grote hoeveelheden verspreid kan worden, leidt tot een meer dynamische en minder overzichtelijke sturingsomgeving. Beslissingen zullen namelijk eerder en sneller genomen kunnen worden. De gevolgen van beslissingen zullen op hun beurt eerder bekend zijn. En reacties op veranderingen zullen eveneens eerder mogelijk en nodig zijn. Turbulentie en de daarbij behorende achteruitgang van sturingscapaciteit, beperkt zich overigens niet tot de overheid. Dit probleem geldt ook voor bedrijven, waardoor een afname van de algemene sturingscapaciteit van samenlevingen het gevolg is.
3. *Complexiteit.* De onderlinge samenhang en de complexiteit van informatieprocessen nemen sterk toe. Ook dit beïnvloedt de sturingscapaciteit van de overheid en die van bedrijven, omdat sturing kennis vereist van de aard en intensiteit van de samenhang in de bestuurde omgeving. Zo zal het moeilijker worden om een adequaat beeld van de economie te krijgen, indien bedrijven vaker delen van hun productie naar het buitenland verplaatsen. Dan bestaat het gevaar dat maatre-

gelen worden genomen op grond van een onvolledig beeld van de werkelijkheid.

4. *Deterritorialisering.* Overheidsingrijpen is gebonden aan een bepaald territoir, informatie niet. Wanneer steeds meer activiteiten op steeds meer plaatsen met elkaar samenhangen, vervagen de grenzen, in de ruimste betekenis van het woord. Steeds meer burgers verrichten hun activiteiten in het buitenland – bijvoorbeeld sparen en gokken – maar de sturingsmacht van de overheid stopt bij de grens. Grote delen van het handelen van burgers en bedrijven zijn zo niet meer door overheden te controleren.
5. *Anarchie.* Het karakter van de nieuwe media wijkt sterk af van dat van de overheid. Internet staat vaak model voor alle nieuwe media. Het Internet wordt dan gekenschetst als fundamenteel onbeheersbaar. Ook wordt wel gewezen op het anarchistisch karakter van de Internet-gebruiker en vervolgens wordt dan geconcludeerd dat de nieuwe informatiesamenleving een gelijksoortig onbeheersbaar en anarchistisch karakter zal hebben. Dit staat haaks op de wens van overheden om maatschappelijke processen te beheersen en de samenleving te ordenen.

De bovenstaande trends en verwachtingen, die in verschillende combinaties en gedaanten in de literatuur over de informatiesamenleving terugkeren, plaatsen de overheid in een wereld die zich qua aard moeilijk laat sturen en waarvan een deel der bewoners zich niet wil laten sturen. Dit staat in scherp contrast met de vroege opvattingen over informatietechnologie. Die werd vooral gedomineerd door de angst dat de met computers uitgeruste overheid een soort elektronisch panopticum zou creëren. Het beeld van de onmachtige overheid wordt op verschillende manieren ingevuld. Voor de Japanse onderzoeker Ohmae geldt de onmacht vooral de nationale staat[1]. Hij constateert dat er een «mismatch» bestaat tussen enerzijds een nieuwe regionale structuur van economische samenhang – Ohmae voorziet sterke economische regio's, zoals Oost-Azië – en anderzijds de besturingseenheid: de natiestaat. Regionale overheden worden in deze visie de nieuwe machtscentra, die de traditionele centra van macht – staten en sommige op nationale staten gebaseerde internationale samenwerkingsverbanden, zoals de Verenigde Naties – zullen verdringen.

Anderen gaan verder en nemen de plotselinge onmacht van de overheid als uitgangspunt voor beschouwingen waar de overheid geheel of gedeeltelijk haar invloed zal verliezen. In de visie van de Franse onderzoeker Lyotard heeft de overheid in een informatiesamenleving geen exclusieve controle over informatie en informatiekanalen. Dit leidt tot een relatieve achteruitgang van positie: doordat de beslissingsmacht samenhangt met de informatie-positie, zal de overheid haar centrale positie moeten delen met andere geïnformeerde beslissers, bijvoorbeeld multinationals[2]. Deze vroege postmoderne visie is op verschillende manieren uitgewerkt. Zo is de Nederlandse bestuurskundige Frissen van mening dat met name de anarchistische, fragmenterende en decentraliserende tendensen van ICT bepalend zullen worden voor onze beleving en ordening, of liever gezegd: «ont-ordening» van de samenleving. De overheid kan dit tij niet keren. Sterker nog, ongewild is zij het slachtoffer van haar eigen wens tot ordening geworden. De wens tot efficiënte sturing leidt tot intensiever gebruik van ICT, terwijl die informatietechnologie nu juist een decentraliserend karakter heeft[3].

Ook de Wetenschappelijke Raad voor het Regeringsbeleid heeft aandacht besteed aan de positie van de overheid in de informatiesamenleving. De voormalige voorzitter van de WRR, J.P.H. Donner concludeerde dat de mogelijkheden voor specifieke sturing door de overheid afnamen[4]. Nijkamp en Ouwersloot (1996) concluderen in een position-paper geschreven voor een WRR workshop: «Informatisering heeft ... vooral tot

[1] Ohmae, K., 1996.
[2] Lyotard, J.-F., 1987.
[3] Frissen, P.H.A., 1996.
[4] In een toespraak voor het Kabelcongres van 5 november 1996.

gevolg dat de economie enerzijds steeds chaotischer wordt met meer producten, minder stabiliteit en zich afspelend op een grotere ruimtelijke schaal. Anderzijds blijkt het zelfregulerend vermogen van de economie ook toe te nemen. Gevolg is dat zowel de mogelijkheid voor als de noodzaak van een regulerende overheid drastisch afnemen». Het beeld van een overheid die haar ordenende en sturende functie niet meer kan uitoefenen, vindt overigens niet alleen gehoor in wetenschappelijke kring. Ook in de media en onder politici heeft deze zienswijze grote invloed.

4.2. De actieve overheid

Haaks op deze visies staat het beeld van de overheid die actief meehelpt de informatiesamenleving vorm te geven. De maatschappelijke verschuivingen als gevolg van de komst van de informatiesamenleving worden in deze analyses niet ontkend, maar de overheid wordt gezien als een actieve participant die greep moet zien te houden op ontwikkelingen. De motiveringen van het gewenste overheidsoptreden lopen uiteen, maar kenmerkend is dat de veranderingen juist extra overheidsinzet en overheidsinvesteringen vergen.

1. *Collectieve goederen zijn een zorg van de overheid.* Een belangrijke reden waarom de overheid door sommigen wordt geacht het voortouw te nemen, ligt in het feit dat een groot deel van de infrastructuur voor de informatiesamenleving collectieve goederen zijn. Er wordt dus een expliciet beroep gedaan op de presterende functie van de overheid[1]. Maar soms wordt van de overheid ook een verregaande sturende betrokkenheid verlangd, met name daar waar het gaat om tot een grote mate van standaardisatie te komen. Dit ter voorkoming van kleine, los van elkaar staande «informatie-eilanden».
2. *De arbeidsmarkt moet door de overheid op peil worden gehouden.* De nieuwe kenniseconomie heeft behoefte aan hooggeschoolde werknemers. Tijdens de overgang van de oude, op industrie gebaseerde, naar een nieuwe, op kennis en diensten gebaseerde economie, worden door automatisering en verplaatsing van delen van de productie naar het buitenland veel werknemers uitgestoten. Deze werknemers worden echter onvoldoende opgenomen in de nieuwe, op kennis gebaseerde economische activiteiten. Hier heeft de overheid een belangrijke taak. Zij moet zorgen voor een geschoold arbeidspotentieel, omdat bedrijven in de kennisintensieve sector onvoldoende investeren in scholing. Dit kan leiden tot problemen voor de economie als geheel, omdat andere landen wel voldoende investeren[2].
3. *Het concurrentievermogen dreigt verloren te gaan.* Het welzijn van landen hangt volgens sommigen af van de mate waarin een land in staat is te concurreren met andere landen[3]. De nieuwe kenniseconomie stelt zoveel eisen aan het productieapparaat, dat bedrijven onmogelijk zelf alle investeringen kunnen doen. De overheid moet krachtige impulsen geven voor investeringen in kennistechnologie, onderzoek en scholing. Ook moet belemmerende wetgeving worden gewijzigd.

Kenmerkend voor de roep om actief overheidsingrijpen is, dat de overheid wordt gevraagd verder te gaan dan alleen ordening en het scheppen van randvoorwaarden. Investeren in scholing en technologie zijn hiervan de belangrijkste. Deze roep is ingegeven door een gevoel van urgentie: als de overheid niets doet, dan verliest Nederland de concurrentiepositie en raakt de economie structureel in het slop.

4.3. De ordenende overheid

Ook bij overheden zelf wordt veel aandacht besteed aan de mogelijke gevolgen van de informatiesamenleving. In de afgelopen jaren heeft dit

[1] Krugman, P., 1994.
[2] Reich, Robert B., 1992.
[3] Porter, Michael E., 1990.

geleid tot het verschijnen van een aantal belangrijke beleidsdocumenten. Deze worden hieronder kort besproken.

Analyse van de groep Bangemann (1994)
Dit document schetst de zichtswijze van de EU in relatie tot de elektronische snelweg. De EU moet volgens dit document vooral het ontstaan van allerlei apart gereguleerde en gesubsidieerde deelmarkten tegengaan. Dit zou moeten worden verwezenlijkt door marktwerking te versnellen en monopolies in de Europese communicatiesectoren af te breken.

Actieprogramma Elektronische Snelwegen (1994)
De Nederlandse overheid vindt dat de marktsector het voortouw moet nemen: «De ontwikkelingslijn wordt vooral bepaald door risicodragende investeringen van de private sector in ontwikkeling en toepassing van nieuwe technologieën, netwerken en diensten en door het zakelijke gebruik van diensten in de openbare sector en het privé-gebruik van consumenten». Een rol van de overheid wordt vooral gezien bij het verzekeren van brede toegankelijkheid, bij ontwikkeling van randvoorwaarden voor markten en bij het scheppen van juridische kaders. De nadruk ligt dus op ordening en niet op de presterende functies van de overheid. De ontwikkeling van de elektronische snelweg als collectief goed wordt zelfs afgewezen: ontwikkeling dient te geschieden door risicodragende investeringen van de marktsector.

G7 conferentie (februari 1995)
De voornaamste aanbeveling van deze conferentie was ook dat de overheid vooral voorwaarden dient te scheppen en zich niet actief moet opstellen. Aan de betrokkenheid van de overheid bij infrastructurele ontwikkeling werd zelfs een duidelijke grens gesteld: alleen pilot- en onderzoeksprojecten en geen concurrentievervalsende overheidsinvesteringen.

Bonn conferentie (1997)
De meest recente Europese conferentie waarop de toekomst van de informatiesamenleving en de rol van overheden werd besproken werd in juli 1997 in Bonn gehouden. Nadruk lag hier eveneens op de taak van overheden om gunstige randvoorwaarden te scheppen.

Op basis van deze documenten kan men een derde visie op de rol van de overheid in de informatiesamenleving schetsen. In deze visie ligt de nadruk sterk op de ordenende functie van de overheid. De overheid moet vooral gunstige randvoorwaarden scheppen voor een verdere ontwikkeling van de informatiesamenleving, zonder daarbij zelf direct het voortouw te nemen. Deze tussenpositie kent de volgende elementen:

1. *De overheid moet kaders bieden voor economische activiteit.* In het algemeen wordt onderkend dat informatietechnologie een belangrijke bron van economische groei kan zijn. Overheden kunnen dienstig kunnen zijn bij het wegnemen van barrières en het scheppen van een passend juridisch kader waarbinnen economische bedrijvigheid ongehinderd kan plaatsvinden.
2. *Verbetering van het eigen functioneren.* Overheden zien in ICT een kans om het eigen functioneren te verbeteren. De dienstverlening ten behoeve van burgers en bedrijven kan met de inzet van de juiste technologische middelen worden verbeterd, terwijl de efficiëntie en de kwaliteit van de dienstverlening kunnen toenemen.
3. *Bescherming van de individuele burger en diens rechten.* Een andere zorg van overheid geldt de plaats van het individu te midden van complexe technologie. Overheden zijn van mening dat waarborgen voor privacy nodig zijn en dat ook sociale en culturele verworvenheden niet het slachtoffer mogen worden van technologische ontwikkelingen. Zo baart de hegemonie van de Engelse taal veel continentale Europese overheden zorgen. De zorg voor economische

ongelijkheid, die het gevolg kan zijn van technologie, de informatie-haves en -have-nots, is ook een probleem dat in overheidskringen aandacht krijgt.

4. *Aanpassing en modernisering van juridische kaders.* Overheden zijn zich terdege bewust van het territorialiteitsprobleem en zijn van mening dat alleen zij dit goed in internationaal overleg kunnen oplossen. Ook op het gebied van auteursrechten en domeinnamen willen zij een leidende rol spelen.
5. *Een leidende rol voor de private sector.* Het belangrijkste uitgangspunt in deze visie is dat de private sector het voortouw moet nemen. De overheid zou vooral randvoorwaarden moeten scheppen. Er is binnen deze visie geen prominente plaats ingeruimd voor overheidsinvesteringen.

Voor de Nederlandse overheid betekent deze visie geen fundamentele breuk. De nadruk lag immers al geruime tijd op het vergroten van de ordenende functie, terwijl presteren en sturen en het bieden van zorg, minder nadruk krijgen.

5. De rol van de overheid in de informatiesamenleving: afweging

Drie visies op de rol van de overheid in de informatiesamenleving strijden om voorrang. Aan de ene kant wordt het «einde» van de overheid aangekondigd; zij is een onmachtig instrument geworden dat haar handelen nog maar moeilijk kan legitimeren. Aan de andere kant wordt de overheid juist nadrukkelijk gevraagd te investeren en het voortouw te nemen bij de ontwikkeling van de infrastructuur.
Overheden en regeringen zelf nemen een middenpositie in. Zij zijn niet onwillig om te investeren, maar liever zien zij dat de private sector het voortouw neemt. De eerste interesse van overheden geldt de zorg voor ordelijk maatschappelijk verkeer op de elektronische snelweg. In de terminologie van Geelhoed: wel ordening, maar geen productie. Wel zorg voor juridische infrastructuren, zoals een goed geordend stelsel van domeinnamen, maar geen aanleg van Internet-backbones.
Het kabinet sluit zich vooralsnog bij deze laatste visie aan. Er wordt niet uitgegaan van een min of meer plotseling optredende onbestuurbaarheid van de samenleving, die voornamelijk te wijten zou zijn aan de komst van de elektronische snelweg. Een plotselinge vermindering van de sturingscapaciteit van de overheid ten gevolge van één oorzaak zou ook een te eenvoudig beeld van de werkelijkheid zijn. Economen kampen al jaar en dag met het probleem dat de economische werkelijkheid maar moeilijk in modellen en getallen is te vangen. Lang voor de komst van ICT en de maatschappelijke gevolgen daarvan, was de economische sturing van de samenleving al een uiterst kwetsbaar experiment, dat ondanks alle beperkingen toch met redelijk succes werd uitgevoerd.
De ontwikkelingen op ICT gebied zijn bovendien niet een volledige breuk met het verleden. Hoewel er vanaf het begin van de jaren '90 veel aandacht bestaat voor Internet en andere, als radicaal gepresenteerde ontwikkelingen, lijkt er toch eerder sprake te zijn van continuïteit. De komst van computers in bedrijven en overheidsorganisaties is immers al in de jaren vijftig begonnen, iets vóór het moment dat in de meeste geavanceerde economieën de dienstensector de leidende economische sector werd. Het was in de jaren '60 al ondenkbaar dat «data-intensieve» organisaties, zoals overheid, banken en verzekeraars, zonder geautomatiseerde systemen werkten. Het Internet dateert van 1968. Het begon als een samenwerkingsverband van de RAND-corporation, universiteiten en bedrijven in de defensiesector. Al in de jaren '70 stond dit Internet voor de gehele wetenschappelijke gemeenschap open. Ook andere computernetwerken van communicerende mainframes werden in die tijd gemeengoed. Computerterminals, die ervoor zorgden dat veel werknemers informatiewerkers werden, waren aan het einde van de jaren

'70 gemeengoed. De jaren '80 brachten de personal computer. Ontwikkelingen op dit gebied zijn dus niet nieuw of onverwacht en veel van wat nu als nieuw wordt gezien, is al ruim van tevoren aangekondigd[1].
Wat echter wel is veranderd, is de komst van een massamarkt voor informatietechnologie, waardoor computers en communicatieapparatuur, die vroeger alleen betaalbaar en bruikbaar waren voor grote organisaties, ook voor het individu beschikbaar zijn gekomen. Ontwikkelingen op het gebied van ICT brengen grote veranderingen teweeg in de manier waarop mensen leven en werken. Evenwel: de fundamentele uitgangspunten van onze samenleving worden niet aangetast. Ideeën over sociale rechtvaardigheid, de inrichting van bestuur en samenleving en ook politieke stellingnames, zijn in wezen niet veranderd. Het voornaamste probleem is juist hoe die uitgangspunten toe te passen in de informatiesamenleving. In die problematiek ligt de uitdaging van het nieuwe, maar is ook de continuïteit terug te vinden.
De informatiesamenleving is, wanneer naar de hierboven geschetste ICT-ontwikkelingen wordt gekeken, al voor een belangrijk deel werkelijkheid geworden. Alleen de laatste fase, de ontwikkeling van massamarkten voor informatietechnologieproducten, is nog niet voltooid. Hoewel deze ontwikkeling grote gevolgen zal hebben en met name de penetratie van informatietechnologie in de samenleving zal vergroten en aan informatietechnologie dus een dominantere positie zal geven, zal vooralsnog geen sprake zijn van verdringing van traditionele communicatiemiddelen. Deel I B van de nota gaat hier dieper op in. De overheid moet echter wel manieren vinden om klassieke principes van de rechtsstaat toe te passen in een elektronische omgeving.
Deze visie op de rol van overheid en wetgever betekent niet dat de overheid geen belangrijke taak meer zou hebben bij het stimuleren van de elektronische snelweg. Dit uitgangspunt kan men reeds terugvinden in het Nationaal Actieplan voor de elektronische snelweg. In dit plan staat centraal de gedachte dat de overheid een ordenende en faciliterende rol heeft. Zij dient de normen en waarden van de rechtsstaat ook in een elektronische omgeving te handhaven en het elektronisch maatschappelijk verkeer zoveel mogelijk te ondersteunen. Dat kan niet alleen langs de weg van wetgeving, maar ook door middel van subsidies en het bieden van ondersteunende voorzieningen.

6. Conclusies en voorstellen

- De analyse dat de huidige ontwikkelingen een radicale breuk met het verleden vormen, wordt niet gedeeld. De informatisering van de samenleving is een langdurig en gestaag proces dat al in de jaren vijftig is begonnen.
- De centrale rol van de overheid met betrekking tot de elektronische snelweg, ligt voorlopig in de sfeer van de ordening. De overheid dient de normen en waarden van de rechtsstaat ook in een elektronische omgeving te handhaven en het elektronisch maatschappelijk verkeer zoveel mogelijk te faciliteren.
- Bij de vervulling van die ordenende rol dient de overheid zich rekenschap te geven van het dematerië̈le, turbulente en internationale karakter van de zich ontwikkelende informatiesamenleving.
- Mocht er echter in de toekomst op bepaalde terreinen sprake zijn van verdringing, waarbij elektronische infrastructuren en diensten volledig in de plaats komen van traditionele middelen van communicatie, dan kan niet worden volstaan met het vertalen van de traditionele normen en waarborgen. Dan zullen er geheel nieuwe normen en kaders moeten worden ontwikkeld.

[1] De informatiemaatschappij, 1983.

C. JURIDISCHE VERKENNINGEN

1. Privaatrecht

1.1. Inleiding

Centraal staat de vraag in hoeverre het privaatrecht ook toepasbaar is in een elektronische omgeving. Hiertoe wordt een beschouwing gegeven over het algemeen deel van het privaatrecht. Daarnaast is een drietal bijzondere deelgebieden van het privaatrecht onderzocht. Allereerst het bewijsrecht, waarvan de toepasbaarheid in de elektronische omgeving van belang is voor de ontwikkeling van de elektronische handel. De vraag naar de privaatrechtelijke aansprakelijkheid van tussenpersonen voor onrechtmatige handelingen op Internet is in het bijzonder van belang omdat veelal niet duidelijk is wie de veroorzaker is van de onrechtmatige handeling en waar deze persoon zich bevindt. Geëindigd wordt met een beschouwing over de toepasbaarheid van het internationaal privaatrecht (ipr) in de elektronische omgeving.

1.2. Het vermogensrecht

De beantwoording van de vraag of het vermogensrecht, in het bijzonder het algemeen deel daarvan, geregeld in de Boeken 3, 5 en 6, technologie-onafhankelijk is, is relevant in verband met de ontwikkeling van de elektronische handel. Vastgesteld wordt of de bestaande wettelijke regeling van het contractenrecht zonder al te grote problemen kan worden toegepast in een elektronische omgeving. Genoemde vraag valt eigenlijk uiteen in drie deelvragen. De eerste is in hoeverre de algemene begrippen van het vermogensrecht technologie-onafhankelijk zijn, dat wil zeggen kunnen worden toegepast in een andere dan de traditionele, «papieren» omgeving. De tweede deelvraag is in hoeverre de wettelijke regeling van het vermogensrecht op specifieke punten belemmeringen bevat voor het gebruik van moderne communicatietechnieken. De derde vraag tenslotte is of de wettelijke bepalingen praktisch toepasbaar zijn in een elektronische omgeving. Denkbaar is immers dat de praktische toepasbaarheid tot dusdanige problemen aanleiding geeft, dat dit tot een wezenlijke belemmering voor het gebruik van elektronisch verkeer leidt.

1.2.1. Enkele algemene begrippen van het vermogensrecht

De basisbegrippen van het vermogensrecht zijn, voor zover hier van belang, in het bijzonder de rechtshandeling, de (verbintenisscheppende) overeenkomst en de wederkerige overeenkomst. Deze zijn in het Burgerlijk Wetboek op een zodanig hoog abstractieniveau geregeld, dat zij kunnen worden toegepast onafhankelijk van de bij de totstandkoming daarvan gebruikte communicatietechniek. Met andere woorden: zij zijn reeds geheel of vrijwel geheel technologie-onafhankelijk.

- Totstandkoming van rechtshandelingen.

Een rechtshandeling vereist een op een rechtsgevolg gerichte wil die zich door een verklaring heeft geopenbaard. Hierin zijn twee elementen te onderscheiden, wil en verklaring. De wil zal in het elektronisch rechtsverkeer dezelfde rol kunnen vervullen als in de huidige situatie. Het gaat hier immers om een geestesgesteldheid van degene die een bepaalde rechtshandeling wil verrichten, hetgeen uiteraard niet aan het gebruik van een bepaalde communicatietechniek is gebonden. Ook waar computers in het geval van zogenaamde electronic data interchange (EDI) «zelfstandig» verklaringen uitbrengen, zal dit in veel gevallen geen probleem opleveren. Dit zal immers in de praktijk te herleiden zijn tot een juridisch relevante wil van een persoon of rechtspersoon, tot uitdrukking gebracht door een of

meer gedragingen, zoals bijvoorbeeld het (doen) programmeren van de computer met het oog op het «zelfstandig» versturen of ontvangen van elektronische boodschappen indien aan bepaalde voorwaarden is voldaan.
Indien een met de verklaring overeenstemmende wil ontbreekt, komt de rechtshandeling niettemin tot stand indien degene tot wie de verklaring was gericht dat niet wist (subjectief) en ook niet behoorde te weten (objectief). Dit kan bijvoorbeeld meebrengen dat, indien een computer ten onrechte de aanvaarding van een bepaalde offerte aan de computer van de wederpartij stuurt (en dus in de bewoordingen van de wetgever de wil van de partij die zich verklaart niet overeenstemt met de uitgebrachte verklaring), desondanks een geldige overeenkomst tot stand komt.
Conclusie is dat geen enkele wettelijke belemmering bestaat voor het langs elektronische weg tot stand komen van rechtshandelingen, mits verklaringen elektronisch kunnen worden uitgebracht.

- Het uitbrengen van verklaringen

Voor de totstandkoming van een rechtshandeling eist de wet dat de wil zich door een verklaring moet hebben geopenbaard. De wet kent dus in beginsel geen beperking ten aanzien van de vraag op welke wijze, of door middel van welk communicatiemiddel die verklaring moet worden overgebracht. Het is dus duidelijk dat ook indien de wil wordt overgebracht door middel van een verklaring in de vorm van bijvoorbeeld een datatransmissie, dit enkele feit niet in de weg kan staan aan het totstandkomen van een geldige rechtshandeling. Uiteraard zal het wel van de omstandigheden van het geval afhangen wat die datatransmissie nu precies geacht kan worden te betekenen. Dit is echter niet anders in een traditionele omgeving, waarin de reikwijdte van een verklaring eveneens moet worden bepaald door uitleg daarvan, waarbij de redelijkheid en billijkheid een belangrijke rol speelt. Ook daar is het immers niet steeds duidelijk wat degene die een verklaring uitbrengt tot uitdrukking heeft willen brengen. Dit hangt, aldus de Hoge Raad, af van wat die partijen in de gegeven omstandigheden over en weer redelijkerwijs daaraan mochten toekennen en van wat zij redelijkerwijs van elkaar mochten verwachten[1]. Verklaringen kunnen dus in elektronische vorm worden uitgebracht. Hoe zit het nu met de verdeling van het risico voor het gebruik van bepaalde communicatiemiddelen?

- Het risico ten aanzien van verklaringen; niet-bereiken van de ontvanger en onjuistheid.

Een tot een bepaalde persoon gerichte verklaring, moet, om haar werking te hebben, die persoon hebben bereikt (de ontvangsttheorie). Het enkele uitbrengen of verzenden van de verklaring is dus niet voldoende, maar anderzijds is het niet nodig dat de ontvanger daadwerkelijk van de verklaring moet hebben kennis genomen. Zoals in de traditionele omgeving in beginsel kan worden aangenomen dat een per post uitgebrachte verklaring de wederpartij heeft bereikt indien de brief bij de ontvanger is bezorgd, zo zou in de elektronische omgeving kunnen worden aangenomen dat een e-mailbericht als verklaring in beginsel haar werking heeft wanneer het in de mail-box van de ontvanger is beland.
De wet bepaalt verder dat degene die het transportmiddel van de verklaring kiest, het risico draagt van het onjuist overbrengen daarvan. Het valt ook hier niet in te zien waarom de risico-verdeling op dit punt anders zou moeten liggen in een elektronische omgeving.
Bedacht dient voorts te worden dat de hier bedoelde wettelijke regels tevens bepalend zijn voor het vaststellen van het tijdstip van totstandkomen van een rechtshandeling. Uit het bovenvermelde volgt dus tevens dat ook dat in een elektronische omgeving kan worden vastgesteld.

[1] HR 13 maart 1981, NJ1981, 635 (CJHB; Haviltex).

- Overige bepalingen ten aanzien van rechtshandelingen

Tenslotte valt nog te wijzen op de privaatrechtelijke leerstukken die betrekking hebben op de rechtshandeling, zoals die inzake nietigheden en vernietigbaarheden, vertegenwoordiging e.d.. Doordat de rechtshandeling zélf technologie-onafhankelijk is geregeld, zal de toepassing van genoemde leerstukken op een elektronisch verrichte rechtshandeling geen bijzondere problemen opleveren.

- De (wederkerige) overeenkomst; toepasselijke regels

Voor de in dit verband belangrijkste categorie rechtshandelingen, de verbintenisscheppende overeenkomsten, geeft de wet aanvullende regels. Een verbintenisscheppende overeenkomst is een meerzijdige rechtshandeling, waarbij een of meer partijen jegens een of meer andere een verbintenis aangaan. Ten aanzien van de wederkerige overeenkomst wordt daaraan toegevoegd dat daarvan sprake is indien elk van beide partijen een verbintenis op zich neemt ter verkrijging van de prestatie waartoe de wederpartij zich daartegenover jegens haar verbindt. Hiervoor geldt derhalve in wezen hetzelfde als voor de rechtshandeling in het algemeen. De abstracte begrippen rechtshandeling, meerzijdigheid, verbintenis en prestatie zijn in een elektronische omgeving even goed bruikbaar als in de traditionele wereld. De bepalingen betreffende (wederkerige) overeenkomsten kunnen zonder bijzondere problemen worden toegepast op overeenkomsten die langs elektronische weg tot stand zijn gekomen. Resteert nog de vraag of een overeenkomst langs elektronische weg tot stand kan komen.

- Totstandkoming van (wederkerige) overeenkomsten

Een overeenkomst komt tot stand door een aanbod en de aanvaarding daarvan. Ook deze bepaling leidt niet tot bijzondere problemen. Zowel het aanbod als de aanvaarding zijn immers rechtshandelingen, waarvoor geldt dat de wil tot uitdrukking moet worden gebracht door een verklaring. In het voorgaande is reeds uiteengezet dat zich ten aanzien van de totstandkoming van rechtshandelingen in een elektronische omgeving geen bijzondere problemen voordoen.

Vastgesteld kan worden dat de in dit verband belangrijke algemene begrippen van het vermogensrecht in het Burgerlijk Wetboek technologie-onafhankelijk zijn geregeld, voornamelijk als gevolg van het hoge abstractieniveau van de wettelijke bepalingen terzake. Hierin is derhalve geen belemmering gelegen voor de (verdere) ontwikkeling van het vermogensrechtelijke elektronisch rechtsverkeer. Dit abstractieniveau van de wettelijke bepalingen is overigens eigen aan de aard van het privaatrecht en kan niet zonder meer worden overgenomen in het publiekrecht, bijvoorbeeld als het gaat om grondrechtenbescherming of strafrecht.

1.2.2. Wettelijke belemmeringen op specifieke punten?

Het bovenstaande laat uiteraard onverlet dat op specifieke punten problemen duidelijk kunnen worden. Zo ligt het voor de hand dat bijvoorbeeld wettelijke vormvereisten voor het verrichten van bepaalde typen van rechtshandelingen, zoals de eis van een geschrift, authentieke of notariële akte een belemmering zullen opleveren voor het elektronisch rechtsverkeer. Immers rechtshandelingen die niet in de door de wet voorgeschreven vorm zijn verricht, zijn in beginsel nietig. Daarnaast kan ook het geval waarin de wet een geschrift weliswaar niet vereist voor de geldigheid van bijvoorbeeld een rechtshandeling, maar aan het ontbreken van een geschrift bepaalde (andere) nadelige gevolgen worden verbonden, bijvoorbeeld op het punt van het bewijsrecht een wezenlijke belemmering betekenen voor het elektronisch rechtsverkeer. Vormvoorschriften kunnen om verschillende redenen in de wetgeving zijn

opgenomen. Veelal zal daaraan een zwaarwegend maatschappelijk belang aan ten grondslag liggen, omdat vormvrijheid het uitgangspunt is van het vermogensrecht. De twee belangrijkste redenen voor vormvoorschriften betreffen de rechtszekerheid en de bescherming van de zwakkere partij, zoals consumenten en werknemers. Het is dan ook de vraag of het steeds mogelijk zal blijken te zijn om, ter bevordering van het elektronisch rechtsverkeer, de belemmering weg te nemen zonder aan de beschermingsratio van de desbetreffende wettelijke bepaling wezenlijk afbreuk te doen. In het kader van het MDW-programma wordt thans onderzoek verricht naar de belemmerende werking van vormvereisten voor de elektronische rechtshandeling. Daarvan maakt tevens deel uit de vraag of vormvereisten moeten worden gehandhaafd en in hoeverre er elektronische pendanten moeten komen van bijvoorbeeld authentieke akten. De resultaten van dit onderzoek zullen eind maart 1998 beschikbaar zijn. Verwacht wordt dat het onderzoek niet leidt tot het afschaffen van vele vormvereisten, aangezien deze nog recentelijk, in het kader van de totstandkoming van het nieuwe Burgerlijk Wetboek, zijn herijkt. Bij eventuele andere concreet gebleken wettelijke belemmeringen zal eveneens worden bezien of deze kunnen worden opgeheven.

Tot slot is van belang Richtlijn 97/7/EG betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten. Deze richtlijn stelt ter bescherming van de consument bij door middel van een techniek voor communicatie op afstand gesloten overeenkomsten (zoals bijvoorbeeld de post, de telefoon, de fax en E-mail) een aantal geharmoniseerde, dwingendrechtelijke minimumregels op punten als informatieverstrekking, herroepingsrecht, nakoming en betaling.

1.2.3. Zijn de wettelijke bepalingen praktisch toepasbaar in een elektronische omgeving?

Uitgangspunt is dat in de elektronische omgeving dezelfde bescherming en rechtszekerheid moet worden geboden als in de traditionele omgeving. Dit uitgangspunt kan in beginsel worden gerealiseerd met behulp van technologie-onafhankelijke regelgeving met een hoog abstractieniveau. Doch bij de toepassing van dergelijke regelgeving in een elektronische omgeving is het denkbaar dat dit onvoldoende is. Met name het vaststellen van de juistheid en daarmee van de betrouwbaarheid van elektronische geuite intenties, verklaringen en documenten kan problematisch zijn door het gemak waarmee deze gewijzigd en gemanipuleerd kunnen worden. Ook de onbekendheid met de identiteit van de wederpartij in de elektronische omgeving kan tot belangrijke problemen aanleiding geven, zoals het niet tijdig kunnen ontdekken en bewijzen van welbewuste misleiding. Vormen van overheidsregulering die ondersteunend werken ten opzichte van het materiële en bewijsrecht, dat op zichzelf in belangrijke mate toereikend is, zijn dan ook van groot belang. Te meer, omdat het voor de ontwikkeling van de elektronische snelweg van wezenlijk belang is dat er ook daadwerkelijk op kan worden vertrouwd dat eenzelfde rechtsbescherming en rechtszekerheid wordt geboden als in de traditionele omgeving.

In deel III D van deze nota wordt aandacht besteed aan de zogeheten Trusted Third Parties (TTP's). Op deze plaats reeds wijst het kabinet op de mogelijkheid ondersteunende regels voor deze organisaties op te stellen die de betrouwbaarheid van TTP's voor gebruikers doet toenemen. Daarbij valt te denken aan een regeling die TTP's erkent indien zij aan bepaalde voorwaarden voldoen. Dergelijke ondersteunende overheidsmaatregelen kunnen een grote bijdrage leveren aan de praktische hanteerbaarheid van het vermogensrecht en het civiele bewijsrecht en daarmee aan de «vraag» naar elektronisch rechtsverkeer.

1.2.4. Stimulering van ontwikkelingen door wetgeving; verband met internationale ontwikkelingen

Uit het voorgaande blijkt dat de huidige vermogensrechtelijke wetgeving in beginsel geen wezenlijke belemmeringen voor elektronisch rechtsverkeer lijkt in te houden. Desalniettemin is de vraag gerechtvaardigd of het ambitieniveau van de wetgever niet hoger zou moeten liggen dan het enkel wegnemen van belemmeringen. Gelet op de potentieel grote economische belangen wordt ervoor gekozen op sommige punten bewust het elektronisch verrichten van rechtshandelingen te bevorderen door middel van wetgeving.
Een stimulerende werking kan uitgaan van het in het algemeen deel van het Burgerlijk Wetboek opnemen van een beperkt aantal bepalingen, die de rechter kan gebruiken als leidraad bij het vormgeven van de rechtsontwikkeling. Het zou dan gaan om bepalingen, vergelijkbaar met de zogenaamde «kapstokbepalingen» over goede trouw, redelijkheid en billijkheid en uitoefening van privaatrechtelijke bevoegdheden in strijd met publiekrecht, opgenomen teneinde de rechter enig houvast te bieden bij het invullen van elders in de wet opgenomen normen, in het bijzonder zogenaamde «open normen». Een voordeel hiervan in het kader van de rechtsontwikkeling is dat naar de bedoeling van de wetgever de genoemde bepalingen niet alleen houvast bieden aan de rechter, maar voor deze ook een zekere motiveringsplicht meebrengen. Anders gezegd: als de wetgever houvast biedt, dient de rechter ook aan te geven in hoeverre daarvan gebruik is gemaakt en, zo niet, waarom niet. Dit kan de eenheid in de rechtsontwikkeling ten goede komen, aangezien de open normen op deze wijze in zoverre onder het bereik van de cassatierechter komen. Teneinde de rechtsonzekerheid over de toepasbaarheid van de vermogensrechtelijke normen te verminderen, zullen bedoelde algemene bepalingen in het Burgerlijk Wetboek opgenomen worden. Alsdan wordt een positieve impuls gegeven aan de ontwikkeling van de elektronische snelweg.

In het bijzonder valt hierbij te denken aan de op 12 juni 1996 door de United Nations Commission on International Trade Law (UNCITRAL) vastgestelde Modelwet on Electronic Commerce. Deze modelwet beoogt nationale wetgevers te voorzien van een set internationaal geaccepteerde (model)regels gericht op het wegnemen van wettelijke belemmeringen en het scheppen van juridische zekerheid voor elektronische handel. De modelwet heeft de steun van de Verenigde Staten.
In zijn beleidsvoornemens van 1 juli 1997 onder de titel «A framework for global electronic commerce» zei de Amerikaanse President Clinton over de modelwet:
«The United States Government supports the adoption of principles along these lines by all nations as a start to defining an international set of uniform commercial principles for electronic commerce.»
De modelwet is gericht op het tot standbrengen van een technologie-onafhankelijke juridische infrastructuur, waarin het gebruik van het elektronische rechtsverkeer geen oneigenlijke voor- of nadelen biedt ten opzichte van de papieren wereld. De modelwet is geschreven voor alle vormen van elektronische handel en kan worden toegepast op alle denkbare moderne communicatietechnieken. Zij is opgezet als een «framework law», die naar behoefte kan worden aangevuld door de implementerende staat.
De modelwet gaat op belangrijke punten uit van de zogenaamde «functional equivalent approach», waarbij ten aanzien van elke belemmering voor het gebruik van de elektronische weg, zoals bijvoorbeeld de eis van een geschrift, dient te worden geanalyseerd wat doel en functie van het desbetreffende vereiste zijn. Op grond van deze analyse immers kan worden vastgesteld hoe deze op gelijkwaardige wijze in een elektro-

nische omgeving kunnen worden gewaarborgd. De modelwet formuleert deze technische eisen niet zelf, aangezien zij dan waarschijnlijk op het moment van haar publicatie reeds zou zijn verouderd. Wat zij doet is het formuleren van abstracte criteria waaraan dergelijke eisen moeten voldoen, willen zij in een elektronische omgeving tot eenzelfde mate van zekerheid leiden als op basis van de bestaande wettelijke regeling in een traditionele omgeving het geval is. Alleen immers wanneer dat het geval is, kunnen zij eenzelfde juridische bescherming genieten en daarmee een volwaardig elektronisch alternatief vormen voor de traditionele weg. De modelwet is voorzien van een handleiding voor de implementatie (Guide to Enactment).
De modelwet bevat een aantal regels die een goed uitgangspunt vormen voor de bovengenoemde algemene bepalingen, zoals die ten aanzien van de noties van «geschrift», «handtekening» en «origineel», alsmede die inzake totstandkoming van overeenkomsten en toerekening van elektronische rechtshandelingen.

1.3. Vermogensrechtelijk elektronisch rechtsverkeer en het bewijsrecht

1.3.1. De uitgangspunten van het civiele bewijsrecht

In privaatrechtelijke gedingen is de rechter in beginsel lijdelijk. Hij mag slechts die feiten en rechten aan zijn beslissing ten grondslag leggen die in het geding te zijner kennis zijn gekomen en zijn komen vast te staan. Wat aan feiten en rechten is gesteld en niet of onvoldoende betwist moet hij in beginsel als vaststaand beschouwen. Het is aan partijen om – waar nodig – bewijs te leveren. De relevantie van het bewijsrecht specifiek voor het elektronisch rechtsverkeer is gelegen in het feit dat een elektronische omgeving niet of nauwelijks «tastbaarheden» kent, hetgeen het leveren van bewijs gecompliceerder kan maken.
De bewijslast in een privaatrechtelijke geding rust op beide partijen; elk zal een deel van de voor de beslissing van de zaak relevante feiten en omstandigheden hebben te bewijzen. Aan deze bewijslast is een bewijsrisico verbonden: wie niet slaagt in het hem opgedragen bewijs, verliest in de praktijk doorgaans de zaak. Het is de rechter die bepaalt hoe de bewijslast precies over de partijen wordt verdeeld.
Hoewel de bewijsvoering in een elektronische omgeving wellicht tot andere vragen aanleiding zal geven dan in een traditionele, lijkt het ook hier niet te gaan om een probleem dat specifiek is voor het gebruik van moderne technologie. Bovendien lijkt er in verband met een tweetal uitgangspunten van het Nederlandse civiele bewijsrecht geen sprake van een bewijsrechtelijke belemmering. In de eerste plaats bestaat een zogenaamd open systeem van bewijsmiddelen, dat wil zeggen dat bewijs kan worden geleverd door alle middelen, tenzij de wet anders bepaalt. Elektronische bewijsmiddelen zijn dus toegelaten. In de tweede plaats is de waardering van het bewijs aan de rechter overgelaten, ook hier weer tenzij de wet anders bepaalt. Deze twee uitgangspunten brengen, in onderling verband bezien, mee dat de rechter een bijzonder grote vrijheid heeft op het punt van het bewijs. Deze vrijheid geeft hem de ruimte in te spelen op de ontwikkelingen inzake het elektronisch rechtsverkeer. In wezen is hiermee de kwestie teruggebracht tot een technische. Indien partijen ervoor zorgen dat zij op het technische vlak de zaken deugdelijk hebben geregeld, mag ervan worden uitgegaan dat de rechter daaraan op het punt van de bewijslevering consequenties zal verbinden. Anders gezegd: zoals er gemakkelijk en minder gemakkelijk te vervalsen papieren documenten zijn en betrouwbare en minder betrouwbare getuigen, zo bestaan er in een elektronische omgeving ook betrouwbare en minder betrouwbare apparaten, technieken en methodieken. Ter ondersteuning van de bewijsvoering kunnen ook TTPs een rol spelen.

1.3.2. Specifieke belemmeringen

Zoals in het materiële vermogensrecht, kunnen ook hier – los van de algemene beginselen – specifieke bepalingen een belemmering vormen voor het gebruik van moderne technologie. Zo is voor bepaalde bewijsmiddelen in de wet vastgelegd wat de bewijskracht daarvan is. Voor een akte en een authentieke akte is bepaald dat deze in bepaalde gevallen dwingend bewijs opleveren, hetgeen betekent dat de rechter het daarin vermelde voor waar moet houden. Verdedigbaar is dat hier sprake is van «discriminatie» van het elektronisch rechtsverkeer, daar het begrip «akte» is gedefinieerd als «een ondertekend geschrift, bestemd om tot bewijs te dienen». Het ligt voor de hand dat het begrip «akte» hiermee is beperkt tot de papieren wereld. Ook deze specifieke belemmeringen maken deel uit van het al eerder genoemde onderzoek in het kader van het eerder genoemde MDW-project «Elektronische Rechtshandeling».

1.3.3. Bewijsovereenkomst

In het bijzonder voor zogenaamde gesloten systemen is de bewijsovereenkomst van groot praktisch belang. De bewijsovereenkomst biedt partijen de mogelijkheid de specifieke problemen van bewijsvoering ten aanzien van in elektronische vorm verrichte rechtshandelingen onderling te regelen, bijvoorbeeld door af te wijken van het wettelijke bewijsrecht. In een zogenaamde open omgeving, zoals bijvoorbeeld Internet, is het uiteraard lastig om met bewijsovereenkomsten te werken, aangezien daarin partijen vóór het totstandkomen van de elektronische rechtshandeling nog geen contact hebben gehad.

1.4. Privaatrechtelijke aansprakelijkheid van tussenpersonen

1.4.1. Inleiding

Vragen omtrent privaatrechtelijke aansprakelijkheid voor onrechtmatige gedragingen op Internet richten zich vooral op de positie van de tussenpersoon (access of service provider). Oorzaak hiervan is dat op Internet veelal niet te achterhalen zal zijn welke persoon achter een onrechtmatige gedraging zit en op welke plaats deze persoon zich bevindt. De tussenpersoon is dan logischerwijs degene waarop de ogen zich richten, omdat deze wel bekend is.

In verband met het begrip tussenpersoon dient eerst het leerstuk van de vertegenwoordiging te worden aangestipt. Onder omstandigheden kan de tussenpersoon aan te merken zijn als vertegenwoordiger van de aanbieder of ontvanger van informatie via het net. De wet bepaalt dat een vertegenwoordiger in beginsel instaat voor het bestaan en de omvang van zijn volmacht. Indien de wederpartij in een dergelijk geval schade lijdt doordat de bevoegdheid geheel of gedeeltelijk blijkt te ontbreken, dan is de tussenpersoon daarvoor dus aansprakelijk en dient hij de wederpartij in de vermogenstoestand te brengen waarin deze zou hebben verkeerd indien hij wél bevoegd zou zijn geweest (positief contractsbelang).

Afgezien echter van dergelijke bijzondere gevallen en gevallen van contractuele aansprakelijkheid, berust de privaatrechtelijke aansprakelijkheid van tussenpersonen op de algemene regeling betreffende onrechtmatige daad, neergelegd in het Burgerlijk Wetboek. Deze kent een algemene norm en fungeert als vangnet voor alle gevallen waarin geen bijzondere regel over aansprakelijkheid geldt (bijvoorbeeld milieuaansprakelijkheid, aansprakelijkheid voor verkeersongevallen, productenaansprakelijkheid). Van aansprakelijkheid is sprake indien is voldaan aan de in de wet genoemde vereisten:

- Onrechtmatige daad.
- Toerekenbaarheid van de daad aan de dader.
- Schade.
- Causaal verband.

Voorts volgt uit de wet dat aansprakelijkheid slechts bestaat voorzover de geschonden norm strekt tot bescherming tegen schade zoals die in concreto is geleden (relativiteitsvereiste).

In de praktijk zal het bij aansprakelijkheid voor onrechtmatige gedragingen van tussenpersonen vooral gaan om belediging, racistische uitingen, (anderszins) onrechtmatige (pers)publicaties, inbreuken op persoonlijkheidsrechten, misleidende of (anderszins) onrechtmatige reclame-uitingen, inbreuk op intellectuele eigendomsrechten of portretrecht, het verspreiden van bedrijfsgeheimen, vormen van oneerlijke concurrentie, niet naleving van het recht ter bescherming van persoonsgegevens (bijvoorbeeld de vergaring en opslag van persoonsgegevens zonder toereikende rechtvaardiging of het ontbreken van passende beveiliging) en dergelijke. Het valt dan ook te verwachten dat vooral zuivere vermogensschade en immateriële schade zal worden geleden en dat het aantonen van causaal verband in voorkomende gevallen een probleem zal zijn, hetgeen een beperkende werking op de aansprakelijkheid zal hebben. Een dergelijke beperkende werking zal ook uitgaan van het relativiteitsvereiste, bijvoorbeeld in de zin dat de zorgvuldigheidsnormen waaraan de tussenpersoon zich in het algemeen heeft te houden niet strekken tot bescherming van illegale gebruikers.

1.4.2. Een toerekenbare onrechtmatige daad

Een drietal typen handelingen kan een onrechtmatige daad opleveren:
- Een inbreuk op een recht (een vermogensrecht, zoals het auteursrecht of een persoonlijkheidsrecht, zoals het recht op privacy).
- Een doen of nalaten in strijd met een wettelijke plicht (bijvoorbeeld een controle- of informatieplicht, of de overtreding van strafrechtelijke normen).
- Een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt (zorgvuldigheidsnormen).

De kwestie van aansprakelijkheid van tussenpersonen zal vooral draaien om de onrechtmatigheidsvraag, hetgeen niet tot bijzondere problemen hoeft te leiden daar de algemene norm technologie-onafhankelijk is geformuleerd: een onrechtmatig doen of nalaten kan ook plaatsvinden in elektronische vorm. Daarbij zal vooral het criterium van de maatschappelijke zorgvuldigheid de rechter voldoende ruimte bieden om rekening te houden met de specifieke omstandigheden van de elektronische omgeving. Deze ruimte heeft de rechter evenzeer waar het gaat om toerekening van de daad aan de dader door de mogelijkheid van toerekening op grond van verkeersopvattingen, waardoor het voor aansprakelijkheid niet steeds nodig is dat aan de aansprakelijke een verwijt kan worden gemaakt. Verschillende factoren zullen aldus in de praktijk hun invloed kunnen hebben, waarbij valt te denken aan:
- De mate van betrokkenheid van de tussenpersoon bij de inhoud van de uiting.
- De mate waarin de tussenpersoon redelijkerwijs controle op en zeggenschap over de uiting kan uitoefenen, waarbij ook technische belemmeringen én mogelijkheden een rol kunnen spelen.
- De wijze waarop de tussenpersoon zich profileert jegens het publiek of de abonnees, waarbij kan worden gedacht aan bepaalde uitlatingen omtrent aard, kwaliteit of betrouwbaarheid van de informatie.
- De vraag of de activiteit van de tussenpersoon een beroeps- of bedrijfsmatig karakter heeft.

Meer in het bijzonder zal de onrechtmatigheidsvraag zich toespitsen op de mate van zorg die van tussenpersonen kan worden gevergd ten aanzien van enerzijds het ontdekken van onrechtmatig materiaal in de via hen doorgegeven informatie en anderzijds aan het daadwerkelijk nemen van stappen daartegen. Bij dit laatste valt bijvoorbeeld te denken aan het waarschuwen van eventuele belanghebbenden of de justitie, het weigeren van doorgifte van dergelijk materiaal of zelfs het eigenmachtig verwijderen daarvan. Hierbij zal de rechter uiteraard tevens aandacht besteden aan de maatschappelijke wenselijkheid van het eventueel eigenmachtig optreden van tussenpersonen in verband met algemeen maatschappelijke belangen, zoals in het bijzonder de vrijheid van meningsuiting en het belang van een vrije pers.

Op dit punt lijkt een vergelijking zinvol met situaties waarmee reeds ervaring in de rechtspraktijk is opgedaan en die in bepaalde opzichten overeenkomsten vertonen met die van de service provider. Te denken valt in het bijzonder aan de uitgever en degene die telefoon- of omroeplijnen ter beschikking stelt. Bij aansprakelijkheid voor de uitgever speelt een rol of hij wetenschap heeft van de onrechtmatige uiting en wat van die uiting de betekenis is en voorts dat de uitgever het besluit tot uitgave neemt. Bij dienstverleners die zich niet met de inhoud van de boodschap bemoeien (telefoonmaatschappij, kabelorganisatie) vloeit aansprakelijkheid doorgaans voort uit niet-nakoming van de verplichting tot dienstverlening (telefoongesprekken mogelijk maken; omroepprogramma"s doorgeven) en zelden uit de inhoud van de getransporteerde boodschap. Kabelorganisaties zijn in het verleden wel aansprakelijk gehouden voor doorgifte van programmas die inbreuk maakten op het auteursrecht (piratenzenders), hetgeen vooral verband hield met hun mogelijkheid doorgifte te verhinderen.

Wellicht valt ook een parallel te trekken met bestaande rechtspraak inzake aansprakelijkheid voor door anderen in het leven geroepen gevaarssituaties. In bepaalde gevallen kan de plicht bestaan om, op straffe van aansprakelijkheid, anderen te waarschuwen voor een waargenomen gevaar of zelfs om de gevaarlijke situatie op te heffen, ook al is men niet zelf voor het ontstaan daarvan verantwoordelijk. Daarvoor is echter in het algemeen nodig dat de ernst van het gevaar dat die situatie voor anderen meebrengt tot het bewustzijn van de waarnemer is doorgedrongen. Het is niet ondenkbaar dat een vergelijkbare situatie zich voordoet voor een tussenpersoon in een elektronische omgeving. Of een dergelijke plicht wordt aangenomen en hoever deze dan gaat, zal afhangen van de omstandigheden van het concrete geval, waarbij valt te denken aan de aard en de ernst van het gevaar, de aard van de relatie met de potentieel benadeelde en de mate van bezwaarlijkheid van waarschuwen of ingrijpen. Wel dient te worden bedacht dat deze rechtspraak is ontwikkeld in verband met situaties waarbij gevaar voor de (lichamelijke) veiligheid van personen bestond, hetgeen in een elektronische omgeving minder goed voorstelbaar is. Het is derhalve niet zeker dat de rechter bereid zal zijn deze gedachtegang ook toe te passen in gevallen waarin bijvoorbeeld schade aan iemands goede naam of omzetschade dreigt.

Wat de rechter in het concrete geval zal beslissen, kan bij de toepassing van open normen lastig worden voorspeld. Er is ook nog nauwelijks rechtspraak over de kwestie van privaatrechtelijke aansprakelijkheid van tussenpersonen op Internet. De meest bekende zaak betrof een geval van auteursrechtinbreuk: de Scientology Church tegen XS4all e.a[1]. Het ging om een zaak tegen 22 service-providers. De vraag was of zij aansprakelijk waren voor het openbaarmaken van auteursrechtelijk beschermd materiaal.

[1] Pres. Rb s-Gravenhage 12 maart 1996, Computerrecht 1996, p. 73–77.

De President bepaalde dat de tussenpersonen niet meer deden dan gelegenheid geven tot openbaarmaken en dat zij in beginsel geen invloed konden uitoefenen op of zelfs maar kennis droegen van datgene wat diegene die via hen toegang tot Internet hadden gekregen, daarop uitdroegen. Om die reden nam de President in beginsel dus geen aansprakelijkheid aan. Dat zou, aldus de President, anders kunnen zijn in een situatie waarin het volstrekt duidelijk is dat een publicatie van een gebruiker onrechtmatig is en waarin redelijkerwijs mag worden aangenomen dat dit ook bij de tussenpersoon bekend is, bijvoorbeeld doordat hij daarop is geattendeerd. Oudere rechtspraak over auteursrechtinbreuk (met betrekking tot de ongewilde doorgifte van piraten-tv-signalen door een kabelorganisatie) is strenger. Algemeen wordt echter aangenomen dat het loutere transport of het louter versterken van signalen geen grond vormt voor aansprakelijkheid voor auteursrechtinbreuken.

1.5. Het internationaal privaatrecht

1.5.1. Inleiding

Internet is wereldwijd: het kent per definitie geen nationale grenzen. Via Internet worden overeenkomsten gesloten, uitgevoerd en betaald, wordt (oneerlijke) reclame gemaakt, privacy geschonden, auteursrechten aangetast. Welk (nationaal) privaatrecht is hierop van toepassing? Het internationaal privaatrecht zal daarop een antwoord moeten geven, zolang er geen wereldwijde eenvormige regelingen van materieel privaatrecht bestaan.

1.5.2. Toepasselijk recht

Internationaal privaatrecht (ipr) is nationaal recht voor internationale verhoudingen. Het ipr van de Europese landen – en vele daarbuiten – heeft als gemeenschappelijk uitgangspunt, dat internationale verhoudingen worden geregeld volgens het nationale recht van het land, waarmee de internationale verhouding de sterkste aanknoping heeft.
Voor een aantal ipr-vragen bestaan uniforme verdragsregels. Het EG-Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomst 1980 (EVO) geeft als hoofdregel, dat op de overeenkomst van toepassing is het recht dat daartoe door partijen gekozen is en bij ontbreken van een dergelijk recht door het recht van het land, waarmee de overeenkomst de nauwste band heeft. Dat zal doorgaans, zo stelt het EVO, het land van vestiging zijn van de persoon die de karakteristieke prestatie levert. Een uitzondering op deze hoofdregel doet zich voor bij consumentenovereenkomsten, waarbij de keuze voor een ander rechtstelsel dan dat van de gewone verblijfplaats van de consument, deze niet kan afhouden van de bescherming die hij geniet naar het recht van zijn gewone verblijfplaats.
Naast deze hoofdregel wordt in het ipr als aanknopingsfactor een (of meerdere) van de volgende factoren gebruikt: de woonplaats, de vestigingsplaats, de gewone verblijfplaats van de ene of de andere partij – of van beide –, de zeer nauwe band van de overeenkomst met een land, de plaats van sluiting van de overeenkomst of van levering of betaling, de plaats waar het (on)roerende goed dat object van een geding is, zich bevindt of waar het betreffende schip is geregistreerd of ingevlagd, de plaats waar de onrechtmatige daad is begaan of waar deze zijn schadelijke inwerking heeft of waar deze verzekerd is.

Zowel Internetovereenkomsten als onrechtmatige daden gepleegd in de Internetomgeving kennen tot nu toe geen specifiek nationale of internationale ipr-regeling. Doordat de rechtsverhoudingen binnen Internet onbepaalbaar zijn naar plaats, het onvoorspelbaar is waar een bericht zal

worden ontvangen en het onduidelijk is langs welke weg het bericht van verzender bij ontvanger gekomen is, komen maar weinig van de gehanteerde aanknopingspunten voor toepassing in aanmerking. Ook factoren als onbekendheid met de persoon van de (ver)koper, de plaats waar deze zich bevindt en de onduidelijkheid of een bepaalde handeling ergens ter wereld een onrechtmatige handeling oplevert, dragen hier voor een belangrijk deel aan bij. Weliswaar is het bij Internet-overeenkomsten gebruikelijk dat de overeenkomst wordt afgesloten via een zogenaamd «click-contract»: door te clicken op een OK-toets op het scherm accepteert de koper de voorwaarden waaronder de verkoper verkoopt. Die voorwaarden bevatten vaak een paragraaf over de bevoegdheid van een bepaalde nationale rechter (of over arbitrage) en over het op de overeenkomst toepasselijke recht. Is de koper consument, dan is de betekenis van de rechtskeuze (en mogelijk ook van de forumkeuze) beperkt, zij wordt immers doorbroken door de consument-beschermende regels van het recht van de koper. Toch zal bij het ontbreken van een specifiek nationale of internationale ipr-regeling de rechter moeten bepalen met welk recht de elektronisch tot stand gekomen overeenkomst de nauwste band heeft en moeten bezien of er reden is de consument-koper de bescherming te geven die hem als doorgaans zwakkere partij toekomt. Indien hij – noch in verdragen noch in zijn eigen wetgeving een bruikbare verwijzingsregel vindt, kan – zo wordt in de literatuur verdedigd – de rechter zijn eigen nationale recht toepassen, omdat van hem een beslissing gevraagd wordt en hij de daarmee gevraagde rechtsbescherming niet mag weigeren.
In de contractuele relatie tussen informant en geïnformeerde, verkoper en koper, speelt de tussenpersoon – de provider – doorgaans geen zelfstandige, onafhankelijke rol. Het nationale recht zal deze contractuele relatie zelfstandig beoordelen; het ipr zal daarbij dat nationale recht aanwijzen. Internet brengt ook hier geen principiële wijziging in het bestaande ipr-systeem.
Ook bij onrechtmatige daden, via Internet verwezenlijkt, kan de rechter het door partijen gekozen recht toepassen. Als die keuze niet is gemaakt, zal de rechter het recht toepassen van het land waar de onrechtmatige daad heeft plaatsgevonden, of van het land waar beide partijen hun gewone verblijfplaats hebben en bij ongeoorloofde mededinging, het recht van het land waar de mededingingshandeling de concurrentieverhoudingen beïnvloed. Ook hier zal de rechter, indien hij geen bruikbare verwijzingsregel vindt, zijn eigen nationale recht kunnen toepassen, omdat van hem een beslissing gevraagd wordt en hij de daarmee gevraagde rechtsbescherming niet mag weigeren.

1.5.3. Rechtsmacht

Omdat elk land in beginsel zijn eigen nationale regels van ipr kent, is het ook belangrijk te kunnen vaststellen van welk land de rechter in een internationaal geval bevoegd is te beslissen. De rechter die bij de zaak wordt betrokken, bepaalt immers aan de hand van zijn eigen ipr het op de zaak toepasselijke recht. De internationale bevoegdheid van de rechter wordt binnen Europa geregeld door het EG Verdrag betreffende de rechterlijke bevoegdheid en de erkenning en tenuitvoerlegging van beslissingen in burgerlijke en handelszaken (EEX)[1] en door het vrijwel EVEX-Verdrag, dat ook de EVA-staten omvat. Het ontbreekt derhalve nog aan een specifieke bevoegdheidsregeling voor Internetconflicten. De Nederlandse rechter zal aan de hand van het bestaande rechtsmachtrecht zijn bevoegdheid moeten bepalen en zo geen andere regel voorhanden is zijn bevoegdheid kunnen baseren op de gewone verblijfplaats van de eisende partij, zoals geregeld in artikel 126, derde lid, Wetboek van Rechtsvordering.

[1] Binnen het werkingsgebied van het EEX bestaat rechtsmacht in geval van onrechtmatige daad niet alleen ter plaatse van de woonplaats/vestigingsplaats van de gedaagde, maar ook daar waar het schadetoebrengende feit zich heeft voorgedaan. Die plaats is in een internationaal geval niet alleen de plaats waar de schadebrengende handeling is verricht, maar ook die waar deze handeling rechtstreeks zijn uitwerking heeft. Bij een onrechtmatige daad via Internet is dus onder andere bevoegd de rechter van de plaats waar het schadebrengende bericht wordt gelezen.

1.5.4. Arbitrage

Door partijen kan worden overeengekomen eventuele conflicten niet aan een rechter voor te leggen, maar aan arbiters. Een belangrijk verschil ten opzichte van het ipr is dat bij arbitrage partijen hun rechtskeuze niet behoeven te beperken tot het recht van een bestaand rechtsstelsel. Zij kunnen ook kiezen voor toepassing van algemene beginselen van het internationaal handelsrecht of zelfs voor besluitvorming op basis van billijkheid. In de internationale handel is arbitrage zeer gebruikelijk en bovendien efficiënt. Ook voor de elektronische handel kan arbitrage uitkomst bieden.

1.6. Conclusies en voorstellen

- De algemene begrippen van het vermogensrecht in het Burgerlijk Wetboek zijn technologie-onafhankelijk en derhalve toepasbaar in de elektronische omgeving.
- Specifieke bepalingen, in het bijzonder vormvoorschriften, kunnen een belemmering opleveren voor de ontwikkeling van het elektronisch rechtsverkeer. In het MDW-project Elektronische rechtshandeling wordt onderzocht of er daadwerkelijke belemmeringen zijn en of moet worden voorzien in elektronische pendanten van (authentieke) akten.
- Waar mogelijk en wenselijk moeten concreet gebleken wettelijke belemmeringen worden opgeheven.
- Het bewijsrecht werpt in het algemeen geen belemmeringen op voor het elektronisch rechtsverkeer. Echter, om het elektronisch verkeer te faciliteren kan het scheppen van extra rechtszekerheid nodig zijn.
- Een juridisch kader voor TTP's, kan ondersteunend werken ten opzichte van het materiële en het bewijsrecht.
- De rechtsontwikkeling op het gebied van het vermogensrechtelijke rechtsverkeer dient wettelijk te worden ondersteund met behulp van algemene bepalingen in het Burgerlijk Wetboek. De UNCITRAL Modelwet dient daarbij als uitgangspunt.
- Nederland dient actief te participeren in het totstandbrengen van eenvormig privaatrecht.
- De aansprakelijkheid van tussenpersonen voor onrechtmatige handelingen op Internet kan worden gebaseerd op de algemene technologie-onafhankelijke onrechtmatige daadsnorm van het Burgerlijk Wetboek. De rechtsontwikkeling kan worden afgewacht. Er is vooralsnog dan ook geen aanleiding een specifieke bepaling op te nemen voor de privaatrechtelijke aansprakelijkheid van tussenpersonen.
- Voor Internetovereenkomsten en onrechtmatige daden gepleegd in de Internetomgeving bestaat geen specifieke nationale of internationale ipr-regeling. Zo lang een dergelijke specifieke regeling nog niet voor handen is, is het gewenst de door Internet gecreëerde internationaal privaatrechtelijke problemen zoveel mogelijk op te lossen aan de hand van de bestaande oplossingscriteria.
- Hoge prioriteit wordt verleend aan het opstellen van Internet-ipr-regels in het kader van de Haagse Conferentie.

2. Bestuursrecht

2.1. Inleiding

De elektronische snelweg heeft gevolgen voor zowel het algemeen deel als de bijzondere delen van het bestuursrecht. Het algemeen deel, grotendeels neergelegd in de Algemene wet bestuursrecht (Awb), omvat algemene regels voor het voorbereiden, verrichten en uitvoeren van rechtshandelingen (besluiten) door het bestuur. Deze regels eisen dat

zowel de rechtshandeling zelf als de belangrijkste stappen in het besluitvormingsproces dat daaraan voorafgaat schriftelijk worden verricht. Nu dit besluitvormingsproces tevens een proces van communicatie tussen overheid en burger is, dringt de vraag zich op in hoeverre het bestuursrecht ruimte biedt of zou moeten bieden om schriftelijke rechtshandelingen te vervangen door elektronische.
De bijzondere delen van het bestuursrecht omvatten de in talloze wetten en andere voorschriften vervatte regulering van allerlei terreinen van de samenleving: van sociale zekerheid tot ruimtelijke ordening en van onderwijs tot financiële dienstverlening. Het deel van het bestuursrecht dat eisen stelt aan het aanbieden van goederen en diensten roept een probleem op: de internationale rechtsmacht. In andere delen van het bestuursrecht doet dit probleem zich niet voor. Grote delen van het bestuursrecht – het ruimtelijk bestuursrecht, een groot deel van het milieurecht, het agrarisch bestuursrecht, het waterstaatsrecht, maar ook openbare orde – en delen van de horecawetgeving – hebben immers betrekking op het gebruik in ruimste zin van in Nederland gelegen onroerend goed en blijven reeds daarom aan het Nederlands grondgebied gebonden. Het sociaal zekerheidsrecht zou als gevolg van de elektronische snelweg vaker te maken kunnen krijgen met internationale verhoudingen, maar biedt daarvoor reeds oplossingen: om aanspraak te maken op een uitkering dient men in beginsel ingezetene van Nederland te zijn of zijn geweest. Voor het ambtenarenrecht, het vreemdelingenrecht of het subsidierecht levert de elektronische snelweg om weer andere reden weinig nieuwe problemen op.

2.2. Besluitvorming en elektronische communicatie

2.2.1. Inleiding

In het verkeer tussen bestuur en burger is papier nog altijd veruit de belangrijkste informatiedrager. Dit is echter in hoog tempo aan het veranderen: vrijwel alle ministeries en provincies en enkele honderden gemeenten, zelfstandige bestuursorganen en waterschappen beschikken inmiddels over eigen web-sites.[1] Tot dusver worden deze web-sites vooral als voorlichtingsmedium gebruikt, maar vanuit de bestuurspraktijk dient zich in toenemende mate de vraag op in hoeverre deze sites ook een rol zouden kunnen spelen bij het voorbereiden en nemen van besluiten. Het gaat dan om vragen als:
- Mag een burger per e-mail een vergunning aanvragen?
- Mag een gemeentebestuur een ontwerp-bestemmingsplan ter inzage leggen door het op zijn web-site te plaatsen?

2.2.2. De schriftelijkheidseis naar huidig recht

Het bestuursrecht onderscheidt een aantal formele stappen in het besluitvormingsproces. De belangrijkste zijn:
- De aanvraag of aangifte.
- Het «horen» van belanghebbenden.
- Het ter inzage leggen van een ontwerp-besluit of andere documenten.
- Het nemen van een besluit.
- Het bekendmaken en mededelen van een besluit.

Het horen van belanghebbende kan naar keuze van de belanghebbende mondeling of schriftelijk geschieden. Nu deze bepalingen de nadruk leggen op de keuzevrijheid van de belanghebbende, moet worden aangenomen dat deze er in beginsel ook voor kan kiezen om zijn zienswijze per e-mail naar voren te brengen. Voor alle andere zojuist onderscheiden handelingen schrijft de wet in beginsel de schriftelijke vorm voor.

[1] Een geordende lijst is te vinden op http://www.minbiza.nl/intro/overheid.html.

De aanvraag en de aangifte zijn twee veel voorkomende handelingen waardoor een burger het besluitvormingsproces formeel op gang brengt. Een aanvraag is een verzoek van een belanghebbende om een besluit bijvoorbeeld een vergunning, uitkering of subsidie te nemen. De Awb eist dat een aanvraag schriftelijk wordt ingediend, tenzij bij wettelijk voorschrift anders is bepaald. Hoewel bedoeld om in bijzondere gevallen mondelinge aanvragen mogelijk te maken, opent deze clausule ook de mogelijkheid om bij wettelijk voorschrift elektronische aanvragen toe te staan.

Naast besluiten op aanvraag zijn er besluiten die het bestuur eigener beweging ambtshalve neemt. Vaak is de burger dan verplicht desgevraagd of op eigen initiatief de voor het nemen van het besluit benodigde gegevens te verstrekken (aangifte)[1]. Voorbeelden zijn de aangifte inkomstenbelasting, de betaling van de omroepbijdrage en de afdracht van loonbelasting, premies werknemersverzekeringen en BTW. Veelal regelt de desbetreffende bijzondere wet dat de aangifte schriftelijk moet worden gedaan. Het belastingrecht kent echter voor een aanzienlijk aantal gevallen de mogelijkheid om met vergunning van de inspecteur elektronisch aangifte te doen.

Naar huidig recht is een bestuursorgaan echter niet verplicht, maar wel bevoegd om elektronische aanvragen en aangiften in behandeling te nemen. Uit oogpunt van rechtszekerheid en zorgvuldigheid dienen daartoe echter nadere voorzieningen te worden getroffen, van bij voorkeur bij wettelijk voorschrift.

Veel bestuursrechtelijke wetten schrijven voor dat bepaalde (ontwerp-)-besluiten of andere documenten voor het publiek ter inzage worden gelegd. De wetgever heeft daarbij gedacht aan papieren documenten. Tegenwoordig is ook denkbaar dat, bijvoorbeeld op een web-site, de documenten in elektronische vorm ter inzage worden «gelegd». Vooralsnog kan dit de «papieren» terinzagelegging niet vervangen, maar slechts aanvullen. Door terinzagelegging op een web-site worden de stukken immers onvoldoende voor het publiek toegankelijk, zolang nog steeds ingezetenen geen toegang hebben tot Internet.

Het bestuursorgaan kan echter zelf in de toegang tot Internet voorzien, bijvoorbeeld door op zijn kantoor of de openbare bibliotheek voor een ieder toegankelijke computers te plaatsen waarmee de documenten kunnen worden geraadpleegd. Er zijn ook gemeenten die experimenteren met «terinzagelegging» via teletekst achter een lokaal TV-kanaal. Aan de verplichting om desgevraagd kopieën van de documenten te verstrekken, kan dan worden voldaan door te vermelden hoe en waar deze kopieën kunnen worden aangevraagd. Gezorgd moet worden dat ook in dit verband de inhoud van het document op het tijdstip van terinzagelegging wordt gefixeerd, omdat aan het tijdstip van terinzagelegging van een document met een bepaalde inhoud vaak rechtsgevolgen zijn verbonden. Dit probleem speelt ook bij de bekendmaking[2] van besluiten. Een besluit dat aan een belanghebbende is gericht, wordt bekend gemaakt door toezending aan die belanghebbende. Hoewel natuurlijk gedacht is aan toezending van een papieren exemplaar, verzet de wettekst zich niet zonder meer tegen toezending per e-mail, indien de belanghebbende zelf een e-mail-adres opgeeft als correspondentieadres. Wel moet de bekendgemaakte tekst dan op zodanige wijze wordt vastgelegd, dat noch het bestuursorgaan, noch de belanghebbende daarin nog wijzigingen kan aanbrengen.

Besluiten die niet tot een of meer belanghebbenden zijn gericht moeten worden bekendgemaakt door publicatie in een blad, dan wel «op andere geschikte wijze». Dit laat enige ruimte voor elektronische bekendmaking, mits het bereik van de elektronische publicatie onder de relevante doelgroep tenminste even groot is als dat van de papieren publicatie. Bovendien eist de rechtszekerheid ook hier, dat de inhoud van het besluit zodanig wordt vastgelegd dat zij niet voor redelijke betwisting vatbaar is.

[1] Dit is dus een ruimer begrip dan het fiscaaltechnische begrip aangifte.

[2] Voor de mededeling van besluiten geldt mutatis mutandis hetzelfde als voor de bekendmaking.

Tot slot: de bekendmaking van algemeen verbindende voorschriften is geregeld in de Bekendmakingswet. Aan de bekendmaking – in beginsel schriftelijk – zijn rechtsgevolgen verbonden. De Bekendmakingswet staat bekendmaking langs elektronische weg niet in de weg; daaraan worden alleen geen rechtsgevolgen verbonden. Aanpassing van de Bekendmakingswet met het oog op de vervanging van de schriftelijke door de eltronische bekendmaking wordt op dit moment niet overwogen. Een apart probleem is dat een besluit dat niet schriftelijk is vastgelegd eigenlijk helemaal geen besluit is. Ingevolge artikel 1:3, eerste lid is slechts een schriftelijke publiekrechtelijke rechtshandeling een besluit. In de wetsgeschiedenis is daaruit afgeleid, dat het bestuur in beginsel[1] verplicht is besluiten op schrift te stellen. Volgens de jurisprudentie is daarbij voldoende, dat bestaan en inhoud van het besluit uit enig schriftelijk stuk blijken. Nu kan een elektronisch vastgelegd besluit natuurlijk te allen tijde worden omgezet in een geschrift door het uit te printen, maar dat is niet voldoende. Daarnaast is ook hier tenminste vereist dat de elektronische vastlegging uit oogpunt van rechtszekerheid gelijkwaardig is aan schriftelijke vastlegging.

2.2.3. Meer mogelijkheden voor elektronische besluitvorming?

De ervaringen met elektronische aangiften in de sfeer van de fiscaliteit tonen aan, dat er geen onoverkomelijke belemmeringen zijn, maar dat wel nadere regelingen en technische voorzieningen noodzakelijk zijn. Het zou bovendien gewenst zijn dat de Awb op termijn meer duidelijkheid zou geven over de gevallen waarin elektronische communicatie wel en niet toelaatbaar is. Elektronische communicatie heeft immers ook belangrijke voordelen. Een elektronisch ter inzage gelegd of bekend gemaakt document is 24 uur per dag toegankelijk, terwijl bij omvangrijke documenten ook elektronische zoekmogelijkheden de toegankelijkheid sterk kunnen verbeteren. Waar grote aantallen aanvragen of aangiften moeten worden verwerkt, kan elektronische verwerking de efficiency en daarmee de snelheid van de besluitvorming verhogen en de administratieve lasten voor burgers en bedrijven beperken. Informatietechnologie biedt voorts mogelijkheden om de klantvriendelijkheid van het bestuur te verbeteren door bijvoorbeeld interactieve hulp bij het invullen van formulieren of systemen die aan de hand van vragenlijsten reeds een indicatie kunnen geven van het naar aanleiding van de aanvraag of aangifte te nemen besluit. De aangiftediskette inkomstenbelasting is daarvan een voorbeeld.
Het kabinet is daarom van oordeel, dat wettelijke belemmeringen voor elektronische besluitvorming waar mogelijk moeten worden weggenomen, uiteraard zonder afbreuk te doen aan essentiële waarborgen voor de rechtszekerheid en de zorgvuldigheid van de besluitvorming. Het is in dit stadium echter nog niet goed mogelijk en, gelet op de snelle technologische ontwikkelingen, ook niet verstandig, om gedetailleerd in de wet neer te leggen aan welke eisen elektronische besluitvorming precies moet voldoen. De Awb dient te worden aangevuld met een experimenteerbepaling opgenomen worden, 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. De Commissie wetgeving algemene regels van bestuursrecht (Commissie Scheltema) zal worden verzocht over de wenselijkheid en inhoud van een dergelijke experimenteerbepaling te adviseren.

2.3. Internationale rechtsmacht

De bijzondere delen van het bestuursrecht reguleren de meest uiteenlopende maatschappelijke activiteiten. Een belangrijk gevolg van de

[1] Een hier niet terzake doende uitzondering geldt voor besluiten die op onmiddellijke uitvoering zijn gericht. Men denke aan het bevel van een politie-agent om zich van een bepaalde plaats te verwijderen.

elektronische snelweg is, dat een deel van deze activiteiten steeds minder aan een bepaalde geografische plaats zijn gebonden[1]. Activiteiten die de wetgever wegens hun effecten op de Nederlandse samenleving heeft willen reguleren, kunnen steeds gemakkelijker buiten het Nederlandse grondgebied plaatsvinden. Via Internet is het in beginsel eenvoudig om vanuit het buitenland activiteiten te verrichten die in Nederland vergunningplichtig of anderszins bestuursrechtelijk gereguleerd zijn. Te denken valt bijvoorbeeld aan het organiseren van kansspelen, het aanprijzen van geneesmiddelen of het aanbieden van financiële diensten. Deze activiteiten kunnen specifiek op Nederland zijn gericht, maar ook als dat niet het geval is, kunnen zij niet te verwaarlozen effecten op de Nederlandse samenleving hebben. Het enkele feit dat bijvoorbeeld kansspelen in de Engelse taal worden aangeboden, is immers voor veel Nederlanders niet of nauwelijks een barrière.
Dit roept de vraag op in hoeverre het Nederlandse bestuursrecht op dergelijke activiteiten kan of moet worden toegepast. Dat is zowel van belang voor de overheid die de activiteiten wil reguleren, als voor de burger die wil weten aan welke regels hij zich moet houden.

Van oudsher is het bestuursrecht in nog sterkere mate dan het strafrecht of het privaatrecht nationaal georiënteerd. Het bestuursrecht kent geen met het internationaal privaatrecht vergelijkbaar stelsel van conflictregels, die aangeven welk nationaal bestuursrecht in internationale verhoudingen van toepassing is. De voornaamste uitzondering is het belastingrecht, dat een uitgebreid netwerk van belastingverdragen kent.
Via Internet kunnen goederen en diensten worden aangeboden. Als dat vanuit een andere lidstaat van de Europese Unie gebeurt, zijn de problemen nog beperkt, omdat regelgeving over goederen en diensten binnen de EU verregaand is geharmoniseerd. Aanbiedingen via Internet kunnen echter in principe vanuit de hele wereld worden gedaan. Uitgangspunt is dat het Nederlandse bestuursrecht slechts geldt op Nederlands grondgebied. Wie buiten Nederland goederen of diensten aanbiedt, is derhalve niet gebonden aan het materiële Nederlandse bestuursrecht. Voor bestuursrechtelijke handhaving bestaan regelingen inzake internationale rechtshulp niet of nauwelijks. Wel is het zo dat veruit de meeste overtredingen van bestuursrechtelijke voorschriften tevens strafbare feiten zijn. Doch de aard van de overtreding rechtvaardigt veelal niet een rechtshulpverzoek. Voor Nederland is het desalniettemin van belang dat bij overtredingen waarmee voor de Nederlandse rechtsorde een zwaarder belang is gemoeid, een succesvol rechtshulpverzoek kan worden ingediend. Indien sprake is van een dergelijke overtreding, dient deze overtreding strafbaar te worden gesteld, waarbij bij de zwaarte van de strafbaarstelling rekening moet worden gehouden met de kans van slagen van een rechtshulpverzoek.

Bij één en ander dient wel onderscheiden te worden tussen enerzijds voorschriften die betrekking hebben op diensten of informatie in de ruimste zin van het woord en anderzijds voorschriften die betrekking hebben op de stoffelijke goederen zelf. Laatstgenoemde voorschriften zijn gewoon van toepassing zodra de goederen Nederland binnenkomen. Dan bestaat er nog een fysieke goederenstroom die als aanknopingspunt kan dienen. De handhaving van dergelijke voorschriften zal echter moeilijker worden als particulieren via Internet op veel grotere schaal dan nu zelf producten zouden gaan importeren. Het is immers niet goed mogelijk de naleving van dergelijke voorschriften bij de consument te controleren. Bij diensten is geen sprake van een fysieke goederenstroom die als aanknopingspunt kan dienen. Zo is voor het optreden als bank, verzekeraar of beleggingsinstelling veelal een vergunning vereist. Elektronsiche diensten zouden het functioneren van dergelijke vergunningstelsels en

[1] In Deel III B wordt uitgebreid ingegaan in op de vraagstukken die de internationaliseringstendens voor de rechtsmacht met zich meebrengt. Dit deel van de nota ziet specifiek op rechtsmachtvragen die betrekking hebben op de bijzondere delen van het bestuursrecht.

daarmee de belangen die deze vergunningstelsels beogen te beschermen, kunnen ondermijnen.

De elektronische snelweg zou hiermee een bedreiging kunnen gaan vormen voor sommige door het Nederlandse economische bestuursrecht beschermde belangen, doordat zij nieuwe vormen van internationalisering van het economisch verkeer mogelijk maakt. Anderzijds mag het bestuursrecht de ontwikkeling van bonafide vormen van elektronische handel ook niet in de weg te staan.

Voorgesteld wordt in bestuursrechtelijke vergunningstelsels voorzieningen op te nemen, die moeten voorkomen dat buitenlandse dienstenaanbieders Nederlands of Europees recht kunnen omzeilen. Deze voorzieningen zullen er voor moeten zorgen dat een buitenlandse aanbieder – wil hij met Nederland elektronische handel drijven – steeds iemand verantwoordelijk stelt binnen de Europese Unie. Over de implicaties van dit voorstel vindt nog nader onderzoek plaats, alsmede een toetsing van de verenigbaarheid van het voorstel met (toekomstige) Europese regelgeving en met (toekomstige) regelgeving van de WTO.

De WTO heeft onder meer regels opgesteld voor de handel in diensten (General Agreement on Trade in Services). Deze regels geven het kader aan voor de liberalisatie van de handel in diensten. Op basis hiervan zijn WTO-landen bindende liberalisatieverplichtingen aangegaan. Ten aanzien van nationale regelgeving zijn ook randvoorwaarden vastgesteld voor bijvoorbeeld nationale vergunningen ten behoeve van de dienstverlening. In principe gelden deze voorschriften dus ook voor elektronisch geleverde diensten. Het is niet uitgesloten dat op dit gebied nieuwe WTO-afspraken nodig zijn. De Europese Commissie zal hiernaar onderzoek doen. Het is wenselijk actief te participeren in de discussie terzake en mogelijke Nederlandse regelgeving daarop af te stemmen.
Voorts kan er bij bestuursrechtelijke overtredingen die vanuit het buitenland kunnen worden gepleegd, naast eventuele bestuursrechtelijke sanctionering ook voor strafrechtelijke sanctionering gekozen worden, zodat er bij belangrijke inbreuken op de Nederlandse rechtsorde tot rechtshandhaving buiten Nederlands grondgebied kan worden overgegaan.

Op de gevolgen van de internationalisering wordt in meer algemene zin ingegaan in Deel III B.

2.4. Conclusies en voorstellen

- De Awb dient te worden aangevuld 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.
- Voorgesteld wordt in bestuursrechtelijke vergunningstelsels voorzieningen op te nemen, die moeten voorkomen dat buitenlandse dienstenaanbieders Nederlands of Europees recht kunnen omzeilen. Die voorzieningen moeten verenigbaar zijn met (toekomstige) regelgeving van de Europese Unie en de WTO.

3. Strafrecht

3.1. Inleiding

Het strafrecht omvat het recht dat regelt wanneer en hoe de overheid straffend jegens burgers kan optreden. Het strafrecht wordt onder-

scheiden in het materiële en het formele strafrecht. Het hoeft geen betoog dat het strafrecht diep kan ingrijpen in de persoonlijke levenssfeer en daardoor aan strenge eisen moet voldoen. De elektronische snelweg beïnvloedt zowel het materiële als het formele strafrecht in aanzienlijke mate. Bij de behandeling van het materiële strafrecht wordt apart aandacht geschonken aan het vraagstuk van de aansprakelijkheid van de tussenpersoon.

3.2. Het materiële strafrecht: algemeen

Strafbare feiten in verband met de elektronische snelweg kunnen in drie categorieën worden onderscheiden:
1. aantasting van het goed functioneren van informatiesystemen
2. vermogensdelicten (fraude)
3. uitingsdelicten.

3.2.1. Functioneren van informatiesystemen

Deze categorie wordt nader onderscheiden in de zogenaamde CIA-delicten, afgeleid van het Engels:
- confidentiality (vertrouwelijkheid van gegevens);
- integrity (integriteit van systemen);
- availibility (ongestoorde beschikbaarheid van gegevens, programmatuur en diensten).

De vertrouwelijkheid van gegevens is vanouds beschermd door de geheimhoudingsplicht van bepaalde beroepsgroepen, zoals ambtenaren, medici en advocaten. De geheimhoudingsplicht van politie-ambtenaren heeft nader gestalte gekregen in de Wet politieregisters. Niet-naleving van enige geheimhoudingsplicht kan strafrechtelijk worden vervolgd op grond van artikel 272 van het Wetboek van Strafrecht. De vertrouwelijkheid van bedrijfsgeheimen heeft vorm gekregen in artikel 273 van het Wetboek van Strafrecht.

De integriteit van informatiesystemen wordt beschermd door een relatief nieuw type van bepalingen. Informatiesystemen zijn immers van relatief recente datum. Het meest sprekende voorbeeld is de bepaling inzake computervredebreuk van artikel 138a van het Wetboek van Strafrecht, gericht tegen het binnendringen in computers of besloten netwerken. Van aantasting van integriteit is reeds sprake wanneer door het hacken onzekerheid is ontstaan of alle gegevens nog ongewijzigd zijn. Denkbaar is dat bij de verdere ontwikkeling van de informatietechniek nadere strafbepalingen nodig zijn gericht op de bescherming van de integriteit van informatiesystemen. Thans is het al mogelijk stromende gegevens – dus tijdens telecommunicatie, buiten de situatie dat zij zijn opgeslagen op een gegevensdrager – te wijzigen. Een daartegen gerichte strafbepaling ligt in de rede. De Minister van Justitie zal daarom onderzoeken of een aanpassing van artikel 350a van het Wetboek van Strafrecht is aangewezen.

De beschikbaarheid van gegevens, programmatuur en diensten is een afzonderlijk beschermwaardig goed. Zo is de inbreuk op het ongestoord functioneren van systemen of voor het publiek algemeen beschikbare informatietechnologische voorzieningen, alsmede de aantasting van de beschikbaarheid van dergelijke systemen of voorzieningen strafbaar gesteld in de artikelen 161 sexies en 161 septies van het Wetboek van Strafrecht. Bij het voorstel voor een nieuwe Telecommunicatiewet worden deze bepalingen aangepast waardoor buiten twijfel wordt gesteld dat ze ook gelden voor de diensten die ISP's aanbieden. Hierdoor is dan onder andere het zogenaamde bombing van E-mailboxen strafbaar. Ook andere

bepalingen richten zich op het behoud van de integriteit van systemen. De artikelen 350a en 350b van het Wetboek van Strafrecht stellen strafbaar het wijzigen van gegevens of het toevoegen van gegevens aan een geautomatiseerd werk. Daarmee is het wijzigen van gegevens die automatisch door het Internetprotocol worden gegenereerd en een aanwijzing geven van de herkomst van een bericht, het spoofen, strafbaar. Voorshands lijken deze bepalingen voldoende technologie-onafhankelijk te zijn geredigeerd.

3.2.2. Vermogensdelicten

Inbreuken op de vermogenspositie van rechthebbenden kunnen ontstaan door fraude. De bestaande bepalingen over oplichting en vervalsing zijn voldoende technologie-onafhankelijk omschreven voor toepassing op de elektronische snelweg. Verder is onder meer strafbaar het wederrechtelijk verkrijgen van via telecommunicatie aangeboden diensten door «valse signalen» (artikel 326c van het Wetboek van Strafrecht), bijvoorbeeld door modems die het mogelijk maken zonder betaling toch de versluierde signalen van betaaltelevisie te verkrijgen. Het tweede lid van artikel 326c stelt het aanbieden van deze modems zelf strafbaar, ook zonder dat het frauduleuze hoofddelict is gepleegd. Daarmee wordt uitvoering gegeven aan de Aanbeveling R (91) 14 van de Raad van Europa over de juridische bescherming van geëncrypteerde televisiediensten.
De Europese Commissie heeft een voorstel gedaan voor een meer algemene juridische bescherming van geëncrypteerde diensten. Het kabinet stelt voor op dit moment geen initiatieven te nemen en het verloop van de Europese discussie af te wachten. In het algemeen worden gegevens slechts strafrechtelijk beschermd, indien zij zijn voorzien van een bijzondere (technische) voorziening. De bescherming van het strafrecht richt zich dan tegen de aantasting van die voorziening. Het product in de vorm van bitjes zelf is vrij. De achtergrond hiervan wordt gevormd door de in het EVRM en de Grondwet gewaarborgde vrijheid om informatie te vergaren en door te geven. Bovendien is het niet goed mogelijk om in het algemeen de eigendom van digitaal opgeslagen informatie te regelen. Deze informatie is immers onbeperkt kopieerbaar en daarmee niet uniek. Alleen in specifieke gevallen wordt hierop een uitzondering gemaakt, wanneer bijvoorbeeld bepaalde vermogensrechtelijke aspecten van informatie om (strafrechtelijke) bescherming vragen. Een klassieke uitzondering wordt gevormd door de strafrechtelijke bescherming van inbreuken op intellectuele eigendom, waarmee met name beperkingen worden opgelegd aan bepaalde vormen van het gebruik van informatie. Een algemene strafrechtelijke bescherming van eigendom van gegevens is echter niet wenselijk, noch mogelijk. Aanbevolen wordt in toekomstige wetgeving:

- de strafrechtelijke bescherming te blijven richten op de technische voorziening die rond informatie is aangebracht, of
- analoog aan het stelsel van intellectuele eigendom het gebruik van informatie te reguleren.

3.2.3. Uitingsdelicten

De uitingsdelicten op het Internet hebben in de publiciteit veel aandacht getrokken. Het meest in het oog springend zijn de kinderpornografie en de racistische literatuur. Onder de noemer uitingsdelichten vallen een heel scala van delicten zoals belediging (artikel 261), het aanbieden van schadelijk materiaal aan kinderen (artikel 240a) en de onverhoedse confrontatie met pornografie (artikel 240). Uitingsdelicten raken aan het grondrecht van vrijheid van meningsuiting. De wetgever heeft bij uitingsdelicten de afweging gemaakt het maatschappelijk schadelijk effect

van de uiting in die gevallen zwaarder te laten wegen dan het genoemde grondrecht.

Sinds de bepalingen over de verspreiding van aanstootgevend materiaal in 1985 uit het Wetboek van Strafrecht zijn gehaald, geldt algemeen het beginsel dat volwassen, mondige burgers zelf kunnen bepalen welke informatie zij tot zich nemen. Voor de overheid is geen taak weggelegd op het terrein van de «goede smaak» of fatsoen. Wel is er voor de overheid een taak weggelegd om gedragingen strafbaar te stellen ter bescherming van derden, zoals kinderen of bepaalde bevolkingsgroepen. Dit uitgangspunt wordt internationaal niet alom gedeeld. Zo is in sommige landen pornografie strafbaar gesteld, omdat het als onfatsoenlijk wordt aangemerkt. De overheid bepaalt aldaar dus wat mensen al dan niet tot zich mogen nemen, ook al is er geen sprake van bescherming van derden.

Vraag is of het beginsel, dat volwassen burgers zelf moeten kunnen bepalen wat zij tot zich nemen, in de toekomst onverkort kan blijven gehandhaafd. De elektronische snelweg leidt er immers toe dat de plaats waarvandaan iemand een uiting verricht minder van belang is. Op enig moment is wellicht een verdergaande strafbaarstelling nodig, ook al zou dit een inbreuk betekenen op de vrijheid van de volwassen burger om zelf te bepalen van welke informatie hij kennis neemt. Zo is bijvoorbeeld denkbaar uitbeeldingen van ernstig seksueel geweld te verbieden. Nederland zal in internationaal overleg een open houding aannemen tegenover de ontwikkeling van internationale normen. Soms zal daarbij aanpassing van Nederlandse normen, die afwijken van de internationale consensus, moeten worden geaccepteerd.

3.3. Het materiële strafrecht: aansprakelijkheid van de provider

De communicatie op de elektronische snelweg roept vragen op over de aansprakelijkheid van tussenpersonen voor uitingsdelicten die op de elektronische snelweg worden gedaan. Buiten kijf daarbij staat dat degene die strafrechtelijk relevant materiaal via de elektronische snelweg aanbiedt een strafbaar feit begaat.

Het Wetboek van Strafrecht stelt het openbaarmaken en verspreiden van bepaalde uitingen strafbaar. Verder worden als medeplichtigen gestraft zij die opzettelijk gelegenheid, middelen of inlichtingen verschaffen tot het plegen van dat feit (artikel 49 van het Wetboek van Strafrecht). Tussenpersonen die beroeps- of bedrijfsmatig informatie doorgeven, kunnen onder omstandigheden als dader of medeplichtige worden aangemerkt. Uitgevers en drukkers genieten daarbij een bijzondere bescherming: kunnen zij desgevraagd de auteur noemen, dan kunnen zij niet worden vervolgd en gaan zij vrijuit (artikelen 53 en 54 van het Wetboek van Strafrecht).
Het grondrecht van de vrijheid van meningsuiting geeft deze personen een geprivilegieerde positie. Ongewenste zelfcensuur moet daarmee worden voorkomen. Aan de andere kant vloeit voor hen uit de artikelen 418 en 419 ook een zorgverplichting voort: zij zijn in een aantal situaties strafbaar als zij geen auteur kunnen aanwijzen. Deze regeling in het Wetboek van Strafrecht is evenwel niet meer op deze tijd toegesneden, waar omroepen, kabelnetexploitanten en Internetproviders tot op zekere hoogte met drukkers of uitgevers vergelijkbare rollen vervullen.

De aansprakelijkheid van Internetproviders heeft de laatste jaren veel aandacht gekregen. De Minister van Justitie stelde zich daarbij op het standpunt dat zij aansprakelijk zijn voor de via hen verspreide strafbare informatie, mits zij (afhankelijk van delictsomschrijving) op de hoogte waren of redelijkerwijs konden zijn van de aard van die informatie.

In het voorontwerp voor een Wet Computercriminaliteit II wordt voorgesteld artikel 53 van het Wetboek van Strafrecht ingrijpend te moderniseren. De volgende aspecten staan daarbij centraal:

- Iedere persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen, dient bij de normale uitoefening van dat beroep of bedrijf de bescherming te genieten die het Wetboek van Strafrecht thans toekent aan uitgevers.
- De tussenpersoon kan alleen worden vervolgd indien hij zijn eigen identiteit of die van de (hoofd)dader niet bekendmaakt ofwel nalaat die handelingen te verrichten die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van verdere verspreiding van de (strafbare) uitingen.
- Deze regeling geldt voor alle professionele tussenpersonen, ongeacht het communicatiemedium (techniekonafhankelijkheid).
- De reikwijdte van de strafwet wordt niet uitgebreid. Dit betekent o.a. dat tussenpersonen alleen aansprakelijk kunnen worden gehouden voor de openbaarmaking of verspreiding van informatie, níet voor informatie-uitwisseling tussen enkele personen in de privésfeer via bijvoorbeeld e-mail.

De aansprakelijkheid die tussenpersonen volgens de strafwet hebben, wordt door deze regeling ingeperkt, niet uitgebreid. In de door het wetsvoorstel Computercriminaliteit II voorgestelde regeling is de tussenpersoon alleen aansprakelijk – en kan hij alleen worden vervolgd – wanneer hij niet voldoet aan de aanmaning van de officier van justitie om die handelingen te verrichten die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van de verdere verspreiding van bepaald, naar het oordeel van de officier van justitie strafbaar materiaal. Van de tussenpersoon worden dus geen preventieve maatregelen geëist, zonder dat er duidelijke aanwijzingen zijn voor de aanwezigheid van strafbaar materiaal. Evenmin wordt van hem gevraagd om bij iedere melding of klacht (van bijv. een klant of een abonnee), dat zich onder de door de tussenpersoon verspreide informatie mogelijk strafbaar materiaal bevindt, onmiddellijk maatregelen te treffen ter voorkoming van de verdere verspreiding van dat materiaal. Of het betrokken materiaal inderdaad strafbaar is, staat immers met zon melding nog niet vast; dit staat primair ter beoordeling van de officier van justitie en de rechter en van de tussenpersoon wordt niet verwacht dat hij op de stoel van de officier van justitie of de rechter gaat zitten.
Bovenstaande laat uiteraard onverlet dat de tussenpersoon, net als iedere andere burger, een eigen «verantwoordelijkheid volgens de»wet heeft, zoals art. 7 lid 1 Grondwet het uitdrukt. Dit betekent dat als de tussenpersoon bij de openbaarmaking of verspreiding van bepaalde informatie onvoldoende zorg betracht en hij weet of redelijkerwijs kan weten dat het om strafbaar materiaal gaat, hij zich mogelijk schuldig maakt aan een verspreidingsdelict of medeplichtigheid daaraan. Op dit punt – wat de *strafbaarheid* betreft – worden aan tussenpersonen geen lichtere of zwaardere eisen gesteld dan aan ieder ander. Met name uit klassieke strafrechtelijke leerstukken als voorwaardelijk opzet en schuld (vergelijk het in veel bestaande uitings- en verspreidingsdelicten voorkomende bestanddeel «redelijkerwijs moeten vermoeden», zie art. 137e lid 1 onder 2 Sr) vloeit voor een ieder in Nederland een zorgplicht voort die meebrengt dat hij zich niet aan strafbaarheid kan onttrekken door de ogen te sluiten voor wat er door zijn handen gaat. Wat de tussenpersoon echter onderscheidt van een gewone particulier en wat hem een beschermde positie geeft, is dat hij ingevolge het wetsvoorstel Computercriminaliteit II een beroep krijgt op een bijzondere *vervolgings*uitsluitingsgrond: als de tussenpersoon achteraf alsnog, op aanmaning van de officier van justitie, maatregelen treft ter voorkoming van de verspreiding van het materiaal,

kan hij niet worden vervolgd, ook al is hij naar de letter van de wet strafbaar.

Tot nog toe heeft de verantwoordelijkheid van de Internetprovider in belangrijke mate gestalte gekregen in het Internet Meldpunt Kinderporno. Het kabinet hecht er belang aan dat deze vorm van zelfregulering wordt uitgebreid tot andere uitingsdelicten en op termijn ook tot andere categorieën tussenpersonen. Het kabinet zal de totstandkoming van die zelfregulering actief bevorderen en aan de strafrechtelijke handhaving prioriteit geven.

3.4. Het formele strafrecht

Het formele strafrecht beschrijft de bevoegdheden van de overheid jegens burgers teneinde het materiële strafrecht te handhaven. Artikel 1 van het Wetboek van Strafvordering legt vast dat strafvordering alleen plaats heeft op de wijze bij de wet voorzien. In het algemeen geldt dat waar de inbreuken op de grondrechten van de burger indringender zijn:
- Er zwaardere criteria gelden voor het hanteren van die bevoegdheden.
- De besluitvorming op een hoger niveau is gelegd.

Daar staat tegenover: waar ernstige strafbare feiten (met name bij georganiseerde criminaliteit) ernstige schade aan de samenleving kunnen aanbrengen, dienen de bevoegdheden ingrijpend te kunnen zijn. Dit laat echter onverlet dat er grondrechtelijke of maatschappelijke redenen voor de wetgever kunnen zijn om niet alle middelen toe te laten.

3.4.1. Bijzondere opsporingsmethoden

Het Wetboek van Strafvordering kent sinds 1993 een afdeling «Onderzoek van telecommunicatie» en een afdeling «Onderzoek van gegevens in geautomatiseerde werken» (artikelen 125f en volgende).
Het kabinet is voornemens deze bevoegdheden binnenkort aan te vullen via de Wet computercriminaliteit II, waarvan het voorontwerp op 15 januari 1998 in consultatie is gegaan. Daarin worden regels gegeven met betrekking tot:
- het vastleggen, ontoegankelijk maken en vernietigen van bepaalde computergegevens ten behoeve van de strafvordering;
- de verplichting tot medewerking aan het ontsleutelen van geëncrypteerde telecommunicatie;
- het onderzoek van e-mail ten behoeve van de opsporing en
- het opsporingsonderzoek op openbare computernetwerken, zoals Internet.

Op 17 juni 1997 is het wetsvoorstel bijzondere opsporingsbevoegdheden aan de Tweede Kamer aangeboden. Enkele daarin geregelde bevoegdheden zijn relevant voor de verdere ontwikkeling van het «digitaal rechercheren»:
- Stelselmatige inwinning van informatie over de verdachte door een opsporingsambtenaar zonder dat kenbaar is dat hij als opsporingsambtenaar optreedt (artikel 126j, wetsvoorstel). Een opsporingsambtenaar kan, op bevel van de officier van justitie, undercover deelnemen aan een newsgroup op het Internet of gebruik maken van Internet Relay Chat (het on-line «babbelprogramma»).
- Opnemen van telecommunicatie en vorderen van verkeersgegevens (artikelen 126m, 126n, 126t en 126u wetsvoorstel), thans geregeld in de artikelen 125f en 125g Wetboek van Strafvordering.
- Opnemen van vertrouwelijke communicatie (ook wel direct afluisteren genoemd, artikelen 126l en 126s wetsvoorstel) is met name van belang in die situaties waarin verdachten gebruik maken encrypted e-mail. Deze bevoegdheid houdt onder meer in dat (onder omstandigheden)

op een toetsenbord van een in een kantoor geplaatste computer een bug geplaatst kan worden, zodat vertrouwelijke communicatie kan worden onderschept, voordat het wordt geëncrypteerd.
- Politiële infiltratie (artikelen 126h en 126p wetsvoorstel). Een opsporingsambtenaar zou via Internet deel kunnen nemen aan een netwerk van personen dat bijvoorbeeld kinderpornografie via het net aanbiedt en verspreidt, teneinde in het belang van de opsporing informatie te vergaren over de herkomst ervan.
- Pseudo-koop of -dienstverlening (artikelen 126i en 126q wetsvoorstel). In het voorontwerp Computercriminaliteit II zal deze bevoegdheid worden aangepast in die zin dat ook de pseudokoop mogelijk is van gegevens afkomstig uit een geautomatiseerd werk door tussenkomst van een openbaar telecommunicatienetwerk, bijvoorbeeld het kopen van kinderporno door een opsporingsambtenaar via Internet.
- «Verkennend onderzoek» (artikel 126 ff, wetsvoorstel), onderzoek naar verzamelingen van personen, om vast te stellen op welke wijze daarbinnen misdrijven die een ernstige inbreuk op de rechtsorde maken, worden beraamd of gepleegd. Het is denkbaar dat bepaalde delen van de Internetgemeenschap onderwerp van een dergelijk verkennend onderzoek zijn, namelijk indien er aanwijzingen zijn dat binnen die delen dergelijke ernstige misdrijven worden beraamd of gepleegd. Het verkennend onderzoek dient ter voorbereiding van de opsporing.

Bij de toepassing van deze opsporingsbevoegdheden op de elektronische snelweg moet evenwel een belangrijk voorbehoud worden gemaakt. Nederlandse opsporingsambtenaren mogen bijvoorbeeld op computernetwerken slechts onderzoek doen voor zover de Nederlandse rechtsmacht reikt. Dit betekent dat zij geen onderzoek mogen doen wanneer de betrokken computers zich kennelijk buiten Nederland bevinden of wanneer er zodanige aanwijzingen zijn dat er een gerede kans is dat dit het geval is. Aangenomen mag worden dat dit slechts uitzondering leidt voor zover de opsporingsambtenaar als ieder ander mag rondkijken op een openbaar netwerk. Op de toepassing van deze bijzondere opsporingsbevoegdheden in internationale computernetwerken en de reikwijdte van de rechtsmacht wordt in Deel III B en Deel III F nader ingegaan.

Bestaande en toekomstige gegevens

Enkele bevoegdheden in het Wetboek van Strafvordering hebben betrekking op het verkrijgen van gegevens die in het verleden zijn opgeslagen. Nauwkeuriger dan tot dusver in de wetgeving het geval is, moet hiervan worden onderscheiden de situatie dat maatregelen worden getroffen om gegevens die in de toekomst beschikbaar komen te vergaren. Een voorbeeld is artikel 125i van het Wetboek van Strafvordering. Dit artikel geeft de rechter-commissaris de bevoegdheid om de uitlevering te vorderen van «gegevens, voor zover deze zijn opgeslagen, worden verwerkt of overgedragen met gebruikmaking van een geautomatiseerd werk». Vraag is of deze bepaling alleen is bedoeld voor het onderzoek van reeds bestaande gegevens, dat wil zeggen gegevens die in het verleden zijn opgeslagen in een computer of dat zij ook basis kan zijn voor het aftappen van gegevensverkeer. Over de strekking van artikel 125i blijkt dus in de praktijk onduidelijkheid te bestaan. Daarom bevat het voorontwerp van een Wet computercriminaliteit II een tekstuele wijziging van die bepaling.

Aanbevolen wordt wettelijke bepalingen zo in te richten dat steeds duidelijk is of deze betrekking hebben op alleen het verleden, dan wel ook op gegevens die eerst in de toekomst ter beschikking komen. Deze aanbeveling vindt mede steun in de Aanbeveling van de Raad van Europa

R (95) 13 over «Problems of criminal law with information technology». Indien het gaat om toekomstige gegevens dient de wet een maximumtermijn te bepalen gedurende welke een bevoegdheid mag worden uitgeoefend. De achtergrond hiervan is dat bij de uitoefening van strafvorderlijke dwangmiddelen ten aanzien van opgeslagen informatie de burger vermeend onrechtmatig optreden onmiddellijk aan de rechter moet kunnen voorleggen, terwijl bij opsporing van toekomstige gevens, zoals de telefoontap, naar de aard van de bevoegdheid deze geheim moet blijven gedurende de toepassing daarvan.

Ook is het van belang een helder onderscheid te maken al naar gelang een bevoegdheid inhoudt dat van een derde medewerking wordt gevraagd aan de opsporing, door de verstrekking van gegevens. Uitgangspunt dient te zijn dat medewerking alleen kan worden gevraagd aan personen of instanties in een bepaalde kwaliteit. In het geval van een dergelijke medewerkingsplicht dient bovendien te worden vermeld wat deze plicht inhoudt: de enkele verstrekking van opgeslagen gegevens, zoals in het geval van artikel 125i, of ook het uitvoeren van bepaalde bewerkingen van deze gegevens. Dit laatste kan van een derde alleen worden verlangd indien de wetgeving daarin expliciet voorziet. Ook hierbij dient te worden onderscheiden tussen het verstrekken van gegevens die betrekking hebben op het verleden en gegevens die betrekking hebben op de toekomst. Voor zover het die laatste gegevens betreft dient duidelijk te zijn of het gaat om gegevens die toch reeds zouden zijn vergaard in het kader van de eigen bedrijfsvoering, dan wel of het andere gegevens betreft, bijvoorbeeld het op verzoek van opsporingsinstanties vergaren van gegevens over de verblijfsplaats van een gebruiker van een mobiel telecommunicatie-apparaat. In dat laatste geval staat de gevensopslag geheel in het kader van de facilitering van de opsporing. Tot dergelijke verplichtingen mag niet lichtvaardig worden besloten. Toch zal ten behoeve van de bestrijding van de georganiseerde criminaliteit onderzoek worden verricht naar de mogelijkheid en wenselijkheid van het op verzoek van opsporingsinstanties vergaren van locatiegevens door telecommunicatie-aanbieders en credit card maatschappijen. Het betreft dan gegevens die niet reeds worden vergaard in het kader van de eigen bedrijfsvoering van deze organisaties.

3.4.2. Randvoorwaarden

De ontwikkelingen in de informatietechnologie openen een baaierd van mogelijkheden om de greep op het individu te vergroten, tegenover een vergelijkbare baaierd voor de criminaliteit om haar werkzaamheden te ontplooien en aan het zicht van de overheid te onttrekken. Dit kan leiden tot een elektronische oorlogsvoering tussen rechtshandhavende autoriteiten en de criminaliteit. Deze dient niet uit de weg te worden gegaan. Voor het overheidsoptreden gelden echter randvoorwaarden.

Artikel 10 van de Grondwet omschrijft het grondrecht van de eerbiediging van de persoonlijke levenssfeer; elders in deze nota komt de uitwerking van dit artikel in de nieuwe Wet bescherming persoonsgegevens uitvoerig aan de orde. Voor de toepassing van opsporingsmethoden betekent artikel 10 Grondwet dat indien daardoor een inbreuk wordt gemaakt op de privacy, dan wel op enig ander grondrecht, daarvoor een basis in de wet is vereist. Dit kan zijn in het Wetboek van Strafvordering, dan wel in bijzondere wetgeving. Voor de opslag van gegevens betekent artikel 10 Grondwet eveneens dat daarvoor een basis in de wet is vereist. Daarin voorzien op dit moment de Wet persoonsregistraties en de Wet politieregisters.
Artikel 4 van de Wet politieregisters bepaalt dat persoonsgegevens slechts mogen worden verzameld en verwerkt voor zover dat noodzakelijk is voor

de goede uitvoering van de politietaak. Er zijn dus grenzen aan de opslag en het gebruik van gegevens, ook indien het gegevens betreft uit open bronnen.

Vanouds is de basis voor het optreden van de politie een verdenking in de zin van artikel 27 van het Wetboek van Strafvordering jegens een bepaalde persoon. De afgelopen jaren hebben geleerd dat dit onvoldoende is. Met het oog op bestrijding van georganiseerde criminaliteit en van zware misdrijven, zijn de CID-registers ingericht. Daarbij worden gegevens bijgehouden omtrent betrokkenen bij ernstige criminaliteit, ook los van de verdenking van een concreet strafbaar feit.

Ook anderszins worden gegevens bijgehouden over burgers die geen verdachte zijn in de zin van artikel 27 van het Wetboek van Strafvordering. Wanneer tips binnenkomen die mogelijk van belang kunnen zijn, kunnen deze worden neergelegd in een register. De gegevens dienen na enige maanden te worden gewist. Dergelijke gegevensverzamelingen over burgers die niet als verdachte of als CID-subject kunnen worden aangemerkt, dienen te worden afgeschermd van andere bestanden.
Dit laat onverlet dat wanneer uit een dergelijk bestand blijkt van een strafbaar feit, daarvan proces-verbaal kan worden opgemaakt, ook al heeft dat niets te maken met het onderzoek met het oog waarop de persoonsgegevens oorspronkelijk zijn verzameld. Evenzeer dient het mogelijk te zijn deze registers op bepaalde individuele personen te bevragen. Volgens de Registratiekamer dient het daarbij te gaan om bevragingen over bepaalde individuen en kan deze bevoegdheid niet worden gebruikt om bestanden te koppelen teneinde strafbare feiten boven water te halen waarvan op voorhand geen enkel vermoeden bestaat.

Het adagium «if there is no crime, there is no investigation» impliceert dat koppelingen van registers waarin onverdachte burgers zijn geregistreerd, voor de politie niet zijn toegelaten. Dit leidt tot een compartimentering van registers voor zover het gaat om registraties van onverdachte burgers. De wetgeving voorziet niet in bevoegdheden om deze compartimentering door een algemene registervergelijking te doorbreken.
Onderzocht wordt of in het Wetboek van Strafvordering een bevoegdheid voor de rechter-commissaris moet worden opgenomen die inhoudt dat in zwaarwegende gevallen over mag worden gegaan tot een algemene vergelijking van registers van verdachte en niet verdachte burgers. Het zou hier om een ingrijpende bevoegdheid gaan, omdat zij zou toestaan dat gegevens worden vergeleken van en kennis wordt vergaard over personen ten aanzien waarvan geen feiten of omstandigheden bekend zijn dat zij zich bezig houden met strafbare feiten. Bovendien zou een dergelijke bevoegdheid, meer dan individuele bevragingen, afbreuk doen aan het beginsel dat registers slechts voor een specifiek doel worden aangelegd en in stand gehouden.
In de wetgeving over het bevragen van bestanden dient daarom steeds een onderscheid te worden gemaakt tussen:
- het bevragen op een bepaalde persoon en
- het bevragen op een op voorhand onbepaalde groep van personen (datamining).

Bij datamining zijn veel verdergaandere beperkingen aan het zoeken nodig. Wel moet de mogelijkheid openblijven dat in zeer ernstige zaken (bijvoorbeeld georganiseerde criminaliteit) volgens passende procedures omvangrijke bestanden, ook wanneer deze zijn aangelegd voor geheel andere doeleinden, kunnen worden bevraagd en gekoppeld. Een goede regeling voor de daarbij verkregen resultaten is daarbij een voorwaarde. Zon regeling houdt in ieder geval in: afscherming en specialiteit in de zin dat de gegevens niet daarna voor andere onderzoeken kunnen worden gebruikt en zodra mogelijk vernietigd.

Er kan reden zijn om ook over onverdachte burgers bepaalde aspecten van hun gedrag te volgen teneinde vast te stellen of zij zich niet schuldig maken aan strafbare feiten. Dit volgen van het gedrag van burgers is veeleer een vorm van toezicht, aangezien er nog geen sprake is van enig strafbaar feit. De desbetreffende bestanden dienen daarom afgescheiden te zijn van die van de politieregisters. Een voorbeeld daarvan is het meldpunt ongebruikelijke transacties (MOT). Alle financiële transacties, ook van onverdachte burgers, die voldoen aan bepaalde criteria worden door de banken gemeld. Indien door vergelijking van deze gegevens met die in het CID-register blijkt dat er bij de melding aan het MOT sprake is van een CID-subject, mogen de financiële gegevens worden verstrekt aan de politie. Cruciaal voor het MOT is dat de verstrekking van gegevens door derden aan het meldpunt is gebaseerd op een wettelijke plicht, zodat privaatrechtelijke aansprakelijkheid van derden wordt vermeden en dat er een waterdicht schot is tussen het meldpunt en de politieregisters.

3.4.3. Medewerking van particulieren

Op basis van artikel 11, tweede lid, Wet persoonregistraties worden thans door opsporingsinstanties gegevens verkregen van derden uit een door hen in stand gehouden persoonsregistratie. Dit artikel is echter niet toegesneden op de situatie waarin in het belang van de opsporing gegevens van derden nodig zijn, omdat het artikel de verantwoordelijkheid voor de afweging of een gegeven kan worden verstrekt, neerlegt bij de derde, die dit echter moeilijk kan beoordelen. Daarom zal op korte termijn het WODC een onderzoek starten naar het verkrijgen van gegevens van derden ten behoeve van de opsporing. Op basis van deze resultaten zal worden onderzocht in welke vorm in het Wetboek van Strafvordering een bevoegdheid moet worden opgenomen die inhoudt dat, anders dan door toepassing van artikel 125i van het Wetboek van Strafvordering, derden verplicht kunnen worden om uit een door hen in stand gehouden persoonsregistraties een gegeven te verstrekken.
Aan een dergelijke verplichting moet worden gekoppeld dat kan worden afgeweken van de normale privacyregelgeving, teneinde te voorkomen dat de gegevensstroom die voorwerp is van het onderzoek wordt beïnvloed. Het gaat hierbij in het bijzonder om het mededeling doen aan geregistreerden. Denkbaar in dit verband is zelfs dat geheimhouding wordt opgelegd aan bijzondere categorieen van personen. Geheimhouding kan echter niet worden opgelegd terzake van:

- Gegevens uit het verleden. Die kunnen immers niet meer worden beïnvloed.
- Gegevens die aan het MOT worden verstrekt, of aan een daarmee vergelijkbare toezichthoudende functie. Dit brengt de opsporing immers niet in gevaar. Dit is vergelijkbaar met de situatie waarin bij iemand huiszoeking is gedaan: deze is vrij de personen te waarschuwen omtrent wie informatie is verzameld.

Een ander denkbaar type medewerkingsplicht heeft betrekking op vooruitbetaalde kaarten voor mobiele telefonie (prepaid cards); burgers worden door deze kaarten moeilijker aftapbaar voor de politie. Denkbaar is daarom van telecommunicatie-aanbieders te verlangen dat zij vooruitbetaalde telecommunicatiekaarten slechts op naam en na behoorlijke identificatie van de betrokkene uitgeven. Vergelijkbare vragen met een veel bredere dimensie doemen op bij de te verwachten komst van de multifunctionele chipcard.

3.5. Conclusies en voorstellen

Het voorontwerp voor een Wet computercriminaliteit II voorziet in een aantal belangrijke aanpassingen van een materieel en formeel strafrecht

aan de elektronische snelweg. Het kabinet streeft ernaar het wetsvoorstel nog in 1998 bij de Tweede Kamer in te dienen.

3.5.1. Conclusies materieel strafrecht

- Het strafrecht beschouwt in het algemeen gedragingen vanuit een maatschappelijke functionaliteit, zonder zich op een bepaalde technische modaliteit in het bijzonder te richten en is daarmee in belangrijke mate technologie-onafhankelijk.
- De bescherming van het strafrecht richt zich tegen de aantasting van de bescherming die rond informatie wordt aangebracht. De informatie zelf is vrij. Het is aan te bevelen in toekomstige wetgeving: de strafrechtelijke bescherming te blijven richten op de technische voorziening die rond informatie is aangebracht.
- Nederland zal in internationaal overleg een open houding aannemen tegenover de ontwikkeling van internationale uitingsdelicten, ook als dat een aanpassing van Nederlandse normen betekent.
- De Minister van Justitie zal onderzoeken of een aanpassing van artikel 350 a van het Wetboek van Strafrecht is aangewezen, teneinde ook wijzigen van stromende gegevens strafbaar te stellen.

3.5.2. Conclusies aansprakelijkheid van de provider

- In het voorontwerp voor een Wet Computercriminaliteit II wordt de strafrechtelijke aansprakelijkheid van de tussenpersoon verduidelijkt: op hem rust de plicht – op straffe van vervolging – om, daartoe gemaand door de officier van justitie, achteraf alle handelingen te verrichten die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van de verdere verspreiding van bepaald, naar het oordeel van de officier van justitie strafbaar materiaal.
- Het kabinet hecht er belang aan dat het Internet Meldpunt Kinderporno wordt uitgebreid tot andere uitingsdelicten en op termijn ook tot andere categorieën tussenpersonen. Het kabinet zal de totstandkoming van die zelfregulering actief bevorderen en aan de strafrechtelijke handhaving prioriteit geven.

3.5.3. Conclusies formeel strafrecht

- Wettelijke bevoegdheden tot het verkrijgen van gegevens worden zo ingericht dat steeds duidelijk is:
  - of deze betrekking hebben op gegevens uit het verleden, dan wel op toekomstige gegevens;
  - of van een derde medewerking wordt gevraagd aan de opsporing, door de verstrekking van gegevens;
  - wat, in het geval van een dergelijke medewerkingsplicht, deze plicht inhoudt: de enkele verstrekking, of ook het uitvoeren van bepaalde bewerkingen van gegevens;
  - of het gaat om gegevens die toch reeds zouden zijn vergaard in het kader van de eigen bedrijfsvoering, dan wel of het andere gegevens betreft.
- Het adagium «if there is no crime, there is no investigation» impliceert dat koppelingen van registers waarin onverdachte burgers zijn geregistreerd, voor de politie niet zijn toegelaten. Wel wordt onderzocht of in het Wetboek van Strafvordering een bevoegdheid voor de rechter-commissaris moet worden opgenomen die inhoudt dat in zwaarwegende gevallen over mag worden gegaan tot een algemene vergelijking van registers van verdachte en niet verdachte burgers.
- Ten behoeve van de bestrijding van de georganiseerde criminaliteit zal onderzoek worden verricht naar de mogelijkheid en wenselijkheid van het op verzoek van opsporingsinstanties vergaren van locatiegegevens

door telecommunicatie-aanbieders en credit card maatschappijen. Het betreft dan gegevens die niet reeds worden vergaard in het kader van de eigen bedrijfsvoering.
- In de wetgeving over het bevragen van bestanden dient een onderscheid te worden gemaakt tussen: het bevragen op een bepaalde persoon en het bevragen op een op voorhand onbepaalde groep van personen (datamining). Bij datamining zijn veel verdergaandere beperkingen aan het zoeken nodig.
- Voor het MOT gelden als randvoorwaarden dat: de verstrekking van gegevens door derden is gebaseerd op een wettelijke plicht en dat er een waterdicht schot is tussen het meldpunt en de politieregisters.
- Onderzocht wordt in welke vorm in het Wetboek van Strafvordering een bevoegdheid moet worden opgenomen die inhoudt dat een derde verplicht kan worden, uit een door hem in stand gehouden persoonsregistratie een gegeven te verstrekken. Aan een dergelijke verplichting moet worden gekoppeld dat kan worden afgeweken van de normale privacyregelgeving.
- Geen afwijking van de normale privacyregelgeving wordt opgelegd terzake van gegevens uit het verleden en gegevens die aan het MOT worden verstrekt, of aan een daarmee vergelijkbare toezichthoudende functie.

4. Bijzondere juridische verkenningen

4.1. Inleiding

De komst van de elektronische snelweg veroorzaakt belangrijke veranderingen binnen een aantal bijzondere rechtsgebieden. In dit hoofdstuk wordt per rechtsgebied aangegeven wat de beïnvloeding van de elektronische snelweg inhoudt en welke initiatieven er tot regelgeving inmiddels zijn, of nog moeten worden genomen.

4.2. Auteursrecht en naburige rechten

4.2.1. Inleiding

De Auteurswet 1912 regelt de bescherming van werken en kent daartoe de auteur van een werk of diens rechtsverkrijger het uitsluitende recht toe van openbaarmaking en verveelvoudiging van dat werk. De Wet naburige rechten beschermt prestaties van uitvoerende kunstenaars, fonogrammenproducenten, filmproducenten en omroeporganisaties en kent rechten toe die overeenstemmen met de rechten uit de Auteurswet. Onder verveelvoudigen wordt onder andere verstaan: het maken, bewerken, vertalen of nabootsen van werken. In de elektronische omgeving gaat het om het vastleggen van werk op elektronische dragers en om verveelvoudigingen tijdens het verkeer van beschermd materiaal in elektronische netwerken. Onder openbaarmaken wordt verstaan: het beschikbaar stellen van werken of prestaties aan een publiek, zoals bijvoorbeeld het uitzenden, het ten gehore brengen, of het aanbieden voor verkoop. In de elektronische omgeving gaat het onder andere om het ter beschikking stellen van beschermd beeld- of geluidmateriaal uit een databank, zoals bij «video-on-demand» of betaal-tv.

4.2.2. Beïnvloeding door de elektronische snelweg

In december 1996 hield de World Intellectual Property Organisation (WIPO) een conferentie over de betekenis van het auteursrecht en de naburige rechten op de elektronische snelweg. Aan de orde kwamen het elektronisch verveelvoudigingsrecht, het elektronisch openbaarmakingsrecht, de bescherming van computerprogrammatuur, de plaats van

elektronische publicatie, bescherming van middelen tot technische beveiliging van werken of prestaties, bescherming van informatie over beheer van elektronische rechten en bescherming van elektronische databanken.

4.2.3. Initiatieven tot internationale en Europese regelgeving

Op de WIPO-conferentie zijn nieuwe verdragen aangenomen over het auteursrecht en de naburige rechten, waarin bepalingen zijn opgenomen voor de elektronische omgeving. Tevens is een verklaring aangenomen dat het auteursrecht en de naburige rechten en de beperkingen daarop, volledig van toepassing zijn op de elektronische snelweg.
Voorts werd bepaald dat «on-demand»-diensten vallen onder het recht tot openbaarmaken en dat computerprogrammatuur wordt beschouwd als een auteursrechtelijk werk. Staten moeten zorg dragen voor regels over technische voorzieningen, die werken en prestaties beschermen en daarnaast voor het geven van informatie over beheer van elektronische rechten. Over het elektronische verveelvoudigingsrecht kon geen overeenstemming worden bereikt. Dit in verband met de onduidelijke gevolgen voor de telecommunicatie-industrie en bibliotheken en de mogelijke invloed op concurrentieverhoudingen.

De Europese Commissie bereidt een richtlijn[1] voor over auteursrecht en naburige rechten in de informatiesamenleving. In deze richtlijn zal vermoedelijk ook een aantal onderwerpen aan de orde komen waarover eerder nog geen overeenstemming werd bereikt, zoals het elektronische reproduktierecht of specifieke beperkingen op de rechten.

4.2.4. Betekenis voor de Nederlandse wetgeving

De Nederlandse wetgeving over auteursrecht en naburige rechten behoeft door toedoen van de informatietechnologische ontwikkelingen geen ingrijpende aanpassing. Verwacht wordt, dat nieuwe technologische ontwikkelingen grotendeels in de bestaande wetten kunnen worden ondergebracht. Niettemin heeft de betekenis van computerprogrammatuur en satellietomroep geleid tot recente wijzigingen van de wetgeving. Dit is toe te schrijven aan EG-richtlijnen.
Voor handhaving van rechten op de elektronische snelweg geldt dat het auteursrecht en de naburige rechten voor een belangrijk deel zijn verankerd in internationale verdragen. In internationaal verband (WIPO,EU) wordt verder gewerkt aan harmonisatie van de relevante regels. Het internationaal privaatrecht, voorzover dat niet reeds in die internationale verdragen is neergelegd, biedt nadere aanknopingspunten voor bepaling van toepasselijk recht of geeft partijen de ruimte daarover zelf regels te formuleren.
Een probleem doet zich voor bij de beperkingen op de rechten die thans nog op technologie-afhankelijke wijze zijn gespecificeerd. Collectieve oplossingen die op dit moment bestaan voor massaal fotokopiëren kunnen niet zonder meer op de elektronische snelweg worden toegepast. Het zogenoemde reprorecht is niet geschikt in een elektronische omgeving, waar geen verschil meer te maken is tussen origineel en kopie. In Deel II A wordt hierop dieper ingegaan. Daarnaast lijken de ontwikkelingen op de elektronische snelweg de afstand tussen rechthebbende en gebruiker te verkleinen, waardoor de mogelijkheid om individuele afspraken te maken wordt vergroot. Contracten tussen bibliotheken en uitgevers zijn daarvan praktijkvoorbeelden.
In een binnenkort te verschijnen notitie van de Minister van Justitie en de Staatssecretaris van Onderwijs, Cultuur en Wetenschappen over de betekenis van het auteursrecht en de naburige rechten voor de nieuwe media, zal meer gedetailleerd worden ingegaan op de gesignaleerde

[1] COM(95)382 def.; COM(96)568 def.

problematiek. Deze notitie is mede bedoeld voor de bepaling van een standpunt bij de onderhandelingen die binnenkort starten over de aangekondigde richtlijn van de Europese Commissie.

4.3. Bescherming persoonsgegevens

4.3.1. Inleiding

De Wet persoonsregistraties[1] (Wpr) geeft uitvoering aan artikel 10 van de Grondwet – recht op privacy – en geeft regels voor de omgang met persoonsgegevens. In deze wet zijn de grondbeginselen opgenomen, zoals die zijn geformuleerd in de «Guidelines on the protection of privacy and transborder flows» van de OESO. Deze grondbeginselen staan ook in het Verdrag van de Raad van Europa ter bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens[2]. Deze grondbeginselen voorzien in voorschriften ten aanzien van de kwaliteit – onder andere juistheid en relevantie – en de verwerking – eerlijk, rechtmatig, doelgebonden, kenbaar enzovoorts – van persoonsgegevens. Daarnaast bevatten de grondbeginselen uitgangspunten met betrekking tot de rechten van geregistreerden, zoals over eventuele inzage, correctie en verwijdering. Met de uitwerking van deze grondbeginselen in de Wpr is beoogd een balans aan te brengen tussen enerzijds degene van wie de gegevens worden verwerkt en anderzijds degene die verantwoordelijk is voor de verwerking.
In aanvulling op de Wpr bestaan er sectorspecifieke privacybepalingen. De Wet politieregisters en enkele andere wetten bevatten een uitputtend privacyregime, waarop de Wpr niet van toepassing is.

4.3.2. Beïnvloeding door de elektronische snelweg

De omvang van de informatiestroom en het gemak waarmee informatie kan worden verkregen, verspreid en verwerkt, maken een exponentiële groei door. Gevolg hiervan is een ongebreidelde verspreiding en bewerking van persoonsgegevens, waarvan de geregistreerde veelal niet op de hoogte is. Laat staan dat hij zijn rechten kan effectueren. In een informatiesamenleving, waarin de techniek een voorname rol speelt, bestaat er bovendien niet altijd een keuze om persoonsgegevens af te staan. Denk bijvoorbeeld aan het gebruik van pinpassen: na een transactie blijven altijd gegevens in digitale vorm achter.

4.3.3. Initiatieven tot Europese regelgeving

De Europese Commissie heeft in de komst van de informatiesamenleving aanleiding gezien nieuwe juridische privacybegrippen te ontwikkelen. Die zijn tot op zekere hoogte technologie-onafhankelijk en zullen minder snel verouderen met de voortschrijding van de techniek. Het voorstel van de Europese Commissie heeft uiteindelijk geresulteerd in de zogenoemde EG-privacyrichtlijn[3], die vóór 23 oktober 1998 in het Nederlandse recht geïmplementeerd moet zijn. Naast deze algemene privacyrichtlijn zullen binnen Europa ook sectorale privacyrichtlijnen worden ontwikkeld. Deze moeten een bijdrage leveren aan verdergaande harmonisering. Als voorbeeld hiervan kan het ontwerp van de EG-richtlijn worden genoemd dat handelt over de bescherming van persoonsgebonden gegevens en van de persoonlijke levenssfeer in het kader van digitale netwerken[4].

4.3.4. Betekenis voor Nederlandse wetgeving

Voor Nederland betekent de Europese privacyrichtlijn, dat de privacywetgeving ingrijpende wijzigingen zal ondergaan: de Wet persoonsregistraties zal worden vervangen door de Wet bescherming persoons-

[1] Stb. 1988, 665.
[2] Trb. 1988, 7.
[3] PbEG 1995, L281.
[4] PbEG 1996, L315.

gegevens (Wbp). Daarnaast moeten enkele bijzondere wetten op bepaalde punten worden aangepast. Het kabinet heeft er voor gekozen de tekst van de richtlijn nagenoeg letterlijk te volgen.
Uitgangspunt in het wetsvoorstel bescherming persoonsgegevens is dat volledige technologie-onafhankelijke wetgeving niet tot de reële mogelijkheden behoort. Wel wordt zoveel mogelijk technologie-onafhankelijke wetgeving nagestreefd. De eerste belangrijke wijziging ten opzichte van de Wpr is de vervanging van het technologie-afhankelijke begrip «persoonsregistratie» door de technologie-onafhankelijke term «gegevensverwerking». Hierdoor is de binding met persoonsregistratie losgelaten en wordt ook het verzamelen van persoonsgegevens onder de werking van de wet gebracht. Immers, de bedreiging van de persoonlijke levenssfeer in de informatiesamenleving bestaat juist uit het grote aantal mogelijkheden om persoonsgegevens buiten medeweten van de betrokkene te verzamelen en te verwerken.
Een andere belangrijke verandering is het loslaten van het begrip «houder», waarvoor «verantwoordelijke», in de plaats is gekomen. Hierdoor is steeds een rechtssubject aanspreekbaar op de verwerking van persoonsgegevens. Een van de algemene doelstellingen van het wetsvoorstel is het vermijden van een situatie waarin personen schade ondervinden van geautomatiseerde gegevensverwerking, zonder dat daar een rechtssubject op kan worden aangesproken.

Transparantie

De regels die zijn gericht op transparantie van gegevensverwerking zijn aangescherpt teneinde de ongecontroleerde verwerking van persoonsgegevens tegen te gaan. Zo moet de geregistreerde altijd over de verwerking worden geïnformeerd, ook wanneer hij redelijkerwijs weet kan hebben van opname van zijn persoonsgegevens. Van deze regel kan worden afgeweken indien:

- de betrokkene al over de betreffende informatie beschikt, of
- het informeren leidt tot een onevenredige inspanning. In een dergelijke situatie moet wel de herkomst van gegevens worden bijgehouden.

Het beginsel van de zogeheten doelbinding is eveneens aangescherpt. De verwerking moet noodzakelijk zijn voor het doel. Voorts zijn de rechten aangevuld van degene van wie de persoonsgegevens worden verwerkt. De betrokkene krijgt het recht van verzet toegekend wanneer hij een gerechtvaardigd individueel belang kan aantonen. In geval van verwerking in de «direct marketing»-branche is dit recht absoluut. Ook openbare registers vallen onder het regime van het wetsvoorstel. Als een openbaar register tot doel heeft informatie te geven, is het achterliggende doel van het register mede bepalend voor de wijze van verstrekking van de persoonsgegevens. Zo rust op de verantwoordelijke de plicht om gegevens bij bijvoorbeeld ontsluiting van een openbaar register via Internet of CD-ROM, adequaat te beveiligen tegen enige vorm van verwerking die in strijd is met het doel van het openbare register. Zo kan de verkoop van het handelsregister op CD-ROM niet op zodanige wijze geschieden dat niet alleen bij een rechtspersoon kan worden gezocht welke bestuurders daarin zeggenschap hebben, maar dat tevens zou kunnen worden gezocht in hoeveel rechtspersonen bepaalde personen betrokken zijn. Het handelsregister beoogt immers niet het antwoord te geven op deze laatste vraag. Deze zoekmogelijkheid dient daarom programmatisch te worden afgeschermd. Dit vloeit voort uit de wettelijke opdracht om persoonsgegevens te beveiligen tegen onbedoelde kennisneming.
Ten behoeve van de handhaving van de Wbp, die primair bij de individuele burger ligt, is aan de Registratiekamer een tweetal handhavingsinstrumenten toegekend: de bestuursdwangbevoegdheid en de bestuurlijke boete. Dit is gebeurd met het oog op de toegenomen kwetsbaarheid

van de positie van de burger door toedoen van de nog altijd groeiende informatietechnologische mogelijkheden voor de verwerking van persoonsgegevens vooral, nu hij veelal niet van de verwerking op de hoogte is.

Verwerking van gegevens buiten de EU

In het wetsvoorstel is rekening gehouden met het internationale karakter van de elektronische snelweg en het gemak waarmee activiteiten buiten de rechtsmacht van staten kunnen worden gebracht. Te denken valt aan het buiten de EU verwerken van gegevens die ook vanuit de EU kunnen worden geraadpleegd. Ingevolge het wetsvoorstel is het daarom een verantwoordelijke, die niet in de EU is gevestigd, verboden gegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt, conform de bepalingen van de Wbp.
De risicoaansprakelijkheid voor de verantwoordelijke is afgezwakt. De verantwoordelijke is niet aansprakelijk mits hij kan aantonen dat hem, aangaande de betreffende onrechtmatigheid, geen verwijt treft.
De groeiende mogelijkheden van datamining – het zoeken naar een op voorhand onbepaalde groep van personen – hebben niet tot een aparte regeling geleid. Daarvoor is gekozen, omdat de regels van onverenigbaar gebruik veelal zullen voorkomen dat met behulp van genoemde techniek persoonsgegevens op onrechtmatige wijze worden verwerkt. Veelal, omdat doorbreking van de doelbinding mogelijk is indien dit noodzakelijk is in het belang van bijvoorbeeld de voorkoming, opsporing en vervolging van strafbare feiten. In Deel II, C-3 wordt op de vergaring van gegevens door de politie nader ingegaan. In de relatie tussen burgers onderling is doeldoorbreking slechts dan mogelijk wanneer dit noodzakelijk is in het belang van de bescherming van de betrokkene of van de rechten en vrijheden van anderen. Een rechtvaardigingsgrond derhalve, die zich niet snel zal voordoen.

In het wetsvoorstel voor een Telecommunicatiewet[1] is een apart hoofdstuk gewijd aan de bescherming van persoonsgegevens en de persoonlijke levenssfeer. Dit is mede ingegeven door de eerder genoemde concept-EG richtlijn over de bescherming van persoonsgebonden gegevens en van de persoonlijke levenssfeer in het kader van digitale netwerken. Om te bewerkstelligen dat abonnees en gebruikers van telecommunicatienetwerken en -diensten in ieder geval steeds op een zekere bescherming van de persoonlijke levenssfeer en van persoonsgegevens aanspraak kunnen maken, wordt een algemene zorgplicht gelegd op de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. De zorgplicht wordt nader ingevuld, voornamelijk met rechten die de abonnee toekomen. Zo krijgt een abonnee het recht om ongespecificeerde nota's te ontvangen, om niet-geïdentificeerde oproepen te weigeren, om zelf te bepalen welke gegevens worden opgenomen in een telefoongids en om zelf te bepalen of en zo ja welke verkeersgegevens mogen worden gebruikt voor commerciële doeleinden. Overigens kunnen ook rechtspersonen in de meeste gevallen aanspraak maken op bescherming van hen betreffende gegevens.

4.4. Artikel 13 Grondwet: brief-, telefoon- en telegraafgeheim

4.4.1. Inleiding

Door de voortschrijdende technologische ontwikkelingen is het huidige artikel 13 Grondwet, waarin het brief-, telefoon- en telegraafgeheim is opgenomen, gedateerd geworden. En de aantallen communicatiemiddelen nemen nog altijd toe. Hoewel een aantal nieuwe communicatiemid-

[1] IIK 25 533.

delen met extensieve interpretatie onder de werking van artikel 13 van de Grondwet kan worden gebracht, past een technologie-afhankelijke bepaling ter bescherming van persoonlijke communicatie niet op de elektronische snelweg. Halverwege het jaar 1997 is dan ook een wetsvoorstel[1] tot wijziging van artikel 13 van de Grondwet aan de Tweede Kamer aangeboden. Het wetsvoorstel heeft veel kritiek opgeleverd, zowel in de Tweede Kamer als daarbuiten. Deze kritiek was veelal ingegeven door de gedachte dat het wetsvoorstel leidt tot een vermindering van de bescherming van post en telefoon. Om deze vrees weg te nemen is het regeringsvoorstel door de Tweede Kamer geamendeerd. In de nieuwe tekst wordt het bestaande brief-, telefoon- en telegraafgeheim op de oude voet beschermd, maar wordt daarnaast bescherming verleend aan daarmee vergelijkbare communicatietechnieken. Deze tekst kan in zoverre technologie-onafhankelijk worden genoemd dat het artikel bescherming zal bieden aan nieuwe communicatietechnieken die in de afgelopen jaren tot ontwikkeling zijn gekomen, èn aan technieken die in de komende jaren nog kunnen ontstaan. Ook gegevens met betrekking tot communicatie (verkeersgegevens) worden voortaan beschermd. Deze nieuwe tekst is op 21 januari 1997 door de Tweede Kamer aanvaard.

4.4.2. Het nieuwe artikel 13

Het nieuwe artikel 13 geeft een uitbreiding van het brief-, telefoon- en telegraafgeheim tot het geheim van daarmee vergelijkbare communicatietechnieken. Niet elke communicatietechniek komt voor bescherming in aanmerking: aansluiting zal moeten worden gezocht bij de uitdrukkelijk geregelde communicatietechnieken, met name post en telefoon. Bepalend is, dat sprake moet zijn van een geheim: de communicatie moet een besloten karakter hebben.

4.4.3. E-mail

Bij de parlementaire behandeling van het nieuwe artikel 13 is naar voren gekomen dat zowel het kabinet als de Tweede Kamer e-mail onder de bescherming van artikel 13 wil brengen. Bijzondere beveiligingsvormen (encryptie) zijn daarbij niet vereist. In de systematiek van artikel 13 is e-mail het meest vergelijkbaar met telefoon, maar vertoont het ook een overeenkomst met post, in die zin dat e-mail evenals post een vorm van uitgestelde communicatie is. Zoals ook het geval is bij het briefgeheim, zal opslag van e-mail tijdens transport, of aan het begin en het einde van het transport, ook onder de bescherming vallen. Aangenomen moet worden dat de bescherming van e-mail onafhankelijk is van het gebruikte transportmiddel (gewone telefoonlijn, ISDN, radio- en televisiekabel).

4.5. Mediarecht

4.5.1. Inleiding

De Mediawet geeft onder andere regels over de verzorging van radio- en televisieprogramma's, de uitzending daarvan door middel van omroepzenders, draadomroepinrichtingen en de steunmaatregelen ten behoeve van persorganen. Dit samenspel van regels beoogt de verscheidenheid van radio, televisie en pers te waarborgen en de samenhang in regelgeving ten aanzien van deze media tot uitdrukking te brengen.
De motieven voor overheidsinterventie op dit terrein zijn de volgende:

- schaarste;
- pluriformiteit;
- ordenen van de concurrentie;
- voorzien in een krachtig en kwalitatief hoogwaardig stelsel van publieke omroep.

[1] IIK 25 443.

Interactieve media, zoals Internet, vallen niet onder de reikwijdte van de Mediawet. Op dit moment wordt voor een aanpassing geen aanleiding gezien, omdat deze media nog niet de hoge verspreidingsgraad hebben van radio en televisie. Daarnaast spelen argumenten voor overheidsinterventie, zoals schaarste en pluriformiteit, nog geen rol. De inhoud van de informatie die via deze media wordt verspreid, is vrij behoudens strafbare uitingen of inbreuken op bijvoorbeeld het auteursrecht. Dan zijn de ter zake geldende bepalingen van het Wetboek van Strafrecht van toepassing. Ten aanzien van deze interactieve media is verder artikel 7 van de Grondwet relevant. Dit artikel regelt het recht van vrijheid van meningsuiting. Het artikel staat geen beperkingen toe als gaat om de nieuwe media. Wel zijn in beperkte mate beperkingen toegestaan ten aanzien van radio en televisie.

4.5.2. Beïnvloeding door de elektronische snelweg

De interactieve media hebben thans nog geen hoge verspreidingsgraad die vergelijkbaar is met die van de radio en televisie. Deze situatie kan veranderen. Met name wanneer de convergentie van technieken doorzet en traditionele media verder worden vermengd met deze nieuwe media, kan het zijn dat het minder zinvol is een onderscheid te maken tussen verschillende soorten media. Dit heeft dan niet alleen consequenties voor de Mediawet, maar tevens voor artikel 7 van de Grondwet, dat technologie-afhankelijk is geformuleerd en geen rekening houdt met het ontstaan van nieuwe media.
Een en ander laat onverlet dat alles over Internet kan worden verspreid, zonder dat daarop een specifieke regeling van toepassing is. Een aanzienlijk probleem vormt de verspreiding van schadelijke inhoud waarop de bepalingen van het Wetboek van Strafrecht niet van toepassing zijn (zie verder 4.5.3).
Tot slot biedt de komst van de elektronische snelweg grote mogelijkheden voor economische groei. Teneinde deze mogelijkheden optimaal te kunnen benutten, is er binnen Europa voor gekozen de telecommunicatiemarkt verregaand te liberaliseren. Deze tendens heeft, naast een grondige herziening van de telecommunicatiewetgeving[1], tevens geleid tot herziening van de Mediawet[2]. Ook daarin worden bepalingen geschrapt, die de ontwikkelingen van nieuwe media onnodig beperken. Een van de gevaren van liberalisering is evenwel het monopoliseren van de informatievoorziening door bijvoorbeeld cross-ownerships. Ter voorkoming hiervan is in de nieuwe Mediawet een zogeheten «Murdoch-bepaling» opgenomen, die de eigendom van FM-frequenties door commerciële radiostations beperkt.

4.5.3. Initiatieven tot Europese regelgeving

Ook op het niveau van de EU bestaat er geen specifieke regelgeving voor schadelijke inhoud die via Internet wordt verspreid. Internet en ook andere interactieve media, vallen namelijk niet onder de EG-richtlijn «Televisie zonder grenzen», waarin – kort gezegd – regels staan over het tijdstip van uitzenden van schadelijke informatie. Gedoeld wordt hierbij vooral op een pornografische of extreem gewelddadige inhoud[3]. Deze richtlijn is inmiddels herzien. Het bereik van de richtlijn wordt niet uitgebreid tot de nieuwe media. De Raad van de Europese Unie wil hierover nog op communautair niveau debatteren. Deze discussie zou moeten worden gevoerd aan de hand van een groenboek, dat binnenkort door de Europese Commissie zal worden gepresenteerd.
De Commissie heeft inmiddels al een ander groenboek opgesteld over de bescherming van minderjarigen en de menselijke waardigheid in de context van audiovisuele en informatiediensten[4]. Ook is een mededeling geformuleerd over illegale en schadelijke inhoud op Internet[5]. Thans

[1] IIK 25 533.
[2] Stb. 1997, 336; deze wet is inwerking getreden op 1 september 1997.
[3] PbEG 1989, L298; PbEG 1997, L202.
[4] COM (96) 483 def.
[5] COM (96)487 def.

wordt binnen het kader van de Raad van Europa een aanbeveling voorbereid over de uitbeelding van geweld in de elektronische media. In de Verenigde Staten is wel getracht de verspreiding van schadelijke inhoud via Internet te reguleren. De wet waarin dit werd getracht, de Communications Decency Act, is door het Supreme Court echter strijdig verklaard met het First Amendment (vrijheid van meningsuiting). Deze uitspraak heeft tot gevolg gehad, dat de inhoud die via Internet wordt verspreid in de Verenigde Staten het recht op de hoogste bescherming geniet die onder het First Amendment mogelijk is, namelijk een bescherming die gelijk is aan de gedrukte media.

4.5.4. Betekenis voor Nederlandse wetgeving

Allereerst voorziet het wetsvoorstel voor een nieuwe Telecommunicatiewet in een nieuwe aanpassing van de Mediawet. Er bestaan in Nederland evenwel geen initiatieven om de schadelijke inhoud te reguleren die via Internet wordt verspreid. In Nederland is blijkens de notitie *Bescherming van jeugdigen tegen schadelijke invloeden van audiovisuele media*[1] het beleidsdoel gericht op een meer effectieve bescherming van jeugdigen. Deze notitie doet meer recht aan de veranderde technische en maatschappelijke situatie en de gewijzigde inzichten over de invloed van audiovisuele media op de opgroeiende jeugd. Teneinde dit doel te bereiken wordt naast regelgeving – onder meer vanwege de grondwettelijke beperkingen – ook gestreefd zelfregulering tot stand te brengen. Deze zelfregulering moet leiden tot een classificatiesysteem voor mediaprodukten, waarbij de overheid als subsidieverlener een stimulerende rol moet spelen. Het is de bedoeling de Wet op de filmvertoningen in te trekken. Om achteraf strafrechtelijk te kunnen optreden in het geval dat schadelijk audiovisueel materiaal aan jeugdigen wordt aangeboden, wordt een aanpassing van art. 240a Sr evenwel noodzakelijk geacht.
Naast zelfregulering zijn andere alternatieven denkbaar, zoals de V-chip, die in de Verenigde Staten wordt voorgeschreven en PICS. Alvorens hiertoe wordt overgegaan, laten de Europese mediaministers eerst nader onderzoek doen naar alternatieve mogelijkheden ter bevordering van de controle door ouders op het kijkgedrag van minderjarigen. Het kabinet hecht aan dit onderzoek en zal waar mogelijk vervolg geven aan de resultaten daarvan. Overigens is het kabinet van mening dat maatregelen die tegen geweld via de audiovisuele media kunnen worden genomen, alleen in Europees verband[2] zin hebben.
Tot slot behoeft artikel 7 van de Grondwet aanpassing aan de technologische ontwikkelingen. Hiertoe vindt nog wel nader onderbouwend onderzoek plaats.

4.6. Telecommunicatie

4.6.1. Inleiding

Thans is de Wet op de telecommunicatievoorzieningen (Wtv) nog geldig. Daarin worden onder andere regels gegeven ten aanzien van telecommunicatie-infrastructuur. Een vergunningenstelsel voor de toegang is hier een voorbeeld van. De Wtv zal echter worden vervangen door de Telecommunicatiewet (Tw), waarvan de behandeling thans in de Tweede Kamer[3] plaatsvindt.

4.6.2. Beïnvloeding door de elektronische snelweg

De zeer snelle ontwikkelingen van de informatietechnologie en de enorme toename van capaciteit en kwaliteit van telecommunicatienetwerken, maken de uitwisseling van grote hoeveelheden gegevens over wereld-

[1] IIK 26 266.
[2] IIK 25 266, nr. 2, p. 13.
[3] IIK 25 533.

wijde netwerken mogelijk. Hierdoor ontstaan vele nieuwe toepassingen en diensten op het gebied van de telecommunicatie. Die kunnen grote gevolgen hebben voor de productiviteit en de economische groei. Om deze tendens te stimuleren voert de overheid een beleid van liberalisering van de markt voor de elektronische dienstverlening. Dit maakt dat belemmeringen voor deze markt moeten worden weggenomen.

4.6.3. Initiatieven tot Europese regelgeving

In het kader van het Europese telecommunicatiebeleid zijn enkele richtlijnen tot stand gekomen die liberalisering en harmonisatie tot doel hebben. De twee belangrijkste richtlijnen hiervan zijn de dienstenrichtlijn[1]en de ONP-richtlijn[2]. De dienstenrichtlijn geeft aan hoe de liberalisering vorm dient te krijgen en heeft tot doel een volledig geliberaliseerde telecommunicatiemarkt per 1 januari 1998. De ONP-richtlijn dient ter begeleiding van de overgang naar volledige concurrentie door de harmonisatie van de kaders die gelden voor de verschillende marktpartijen en overheden.

4.6.4. Betekenis voor Nederlandse wetgeving

Vanwege de noodzaak tot liberalisering en tot het wegnemen van belemmeringen voor de ontwikkeling van de markt, was een herziening van de telecommunicatieregelgeving noodzakelijk. De Wtv uit 1989 is qua concept al verouderd, ondanks de vele wetswijzigingen die elkaar in hoog tempo opvolgden. Een ander oogmerk van de herziening van de regelgeving is de uitvoering van EG-richtlijnen betreffende liberalisering en harmonisatie van de telecommunicatiesector. De dienstenrichtlijn en de ONP-richtlijn worden in de Tw geïmplementeerd. In de Tw maakt de toegangsregulering plaats voor gedragsregulering. Waar in de Wtv de nadruk vooral op de infrastructuur lag, legt de Tw het accent op de diensten, de tweede laag in het lagenmodel dat in Deel I B van deze nota wordt gepresenteerd.
De in de Tw gebruikte interventietechnieken zijn minder zwaar dan die in de Wtv. Zo wordt de eis voor het hebben van een vergunning voor toegang tot de infrastructuur in belangrijke mate afgezwakt. Meer wordt overgelaten aan zelfregulering door marktpartijen.

De doelstellingen van de Tw zijn:
- Het versterken van de concurrentiepositie van Nederland door middel van eersteklas telecommunicatievoorzieningen en toepassingen.
- Hoge kwaliteit en grote toegankelijkheid van de telecommunicatie-infrastructuur – bijvoorbeeld door verplichting tot interconnectie en door het stellen van technische eisen voor apparatuur en toegangsspecificaties – zodat er voldoende normalisatie optreedt.
- Het bewaken van maatschappelijke belangen bij de toegang tot en het gebruik van telecommunicatievoorzieningen – zoals universele dienstverlening, bescherming persoonlijke levenssfeer, staatsveiligheid en openbare orde.

In de structuur van de Tw zijn globaal drie categorieën regels te onderscheiden:
– *de toetreding tot de markt*
Voor toetreding tot de markt dienen zo min mogelijk belemmeringen te bestaan. Voor toetreding is niet langer een vergunning vereist, maar een bepaalde vorm van registratie. De overheid heeft wel een ordenende en verdelende taak bij de beschikbaarstelling van specifieke voorzieningen voor telecommunicatie. Het gaat hierbij onder meer om de verdeling en het gebruik van frequenties en de toewijzing van het gebruik van

[1] PbEG 1990, L192.
[2] PbEG 1990, L192.

nummers ten behoeve van openbare telecommunicatiediensten. Nieuw daarbij is een bepaling over nummerportabiliteit.

– *regels voor marktgedrag*

Deze regels betreffen het waarborgen van de beschikbaarheid en kwaliteit van bepaalde vormen van dienstverlening en het stimuleren van marktwerking in de telecommunicatiesector. Dit laatste wordt verwezenlijkt door het toestaan van concurrentie in alle onderdelen van de telecommunicatiemarkt. Daarnaast zijn er echter specifieke regels nodig om concurrentie daadwerkelijk tot stand te brengen. Dit hangt samen met het feit dat in het verleden slechts in beperkte mate concurrentie was toegestaan. Hierdoor heeft de oude monopolist, KPN, een belangrijke voorsprong op nieuwkomers op de markt. Deze marktpartij wordt verplichtingen opgelegd om aan andere marktpartijen en afnemers op een transparante, objectieve en non-discriminatoire wijze en tegen redelijke tarieven toegang te bieden tot hun netwerken en diensten (interconnectie en bijzondere toegang).

– *maatschappelijke belangen*

Ook in een geliberaliseerde telecommunicatiemarkt zijn ter bescherming van het algemeen maatschappelijk belang regels nodig. Hierbij valt te denken aan universele dienstverlening, die bepaalde basisvoorzieningen voor telecommunicatie voor iedere burger tegen redelijke tarieven beschikbaar maakt. De basisvoorzieningen bestaan uit: vaste spraaktelefoniedienst – waarbij ook faxverkeer en telecommunicatie via een modem mogelijk is – en voldoende openbare telefooncellen, gratis toegang tot alarmnummers en beschikbaarheid van telefoongidsen. Een ander aspect dat in dit verband een rol speelt is de bescherming van de persoonlijke levenssfeer.[1] Deze wordt vorm gegeven door middel van een zorgplicht die de aanbieders wordt opgelegd. Ook mag het gedrag van marktpartijen niet ten koste gaan van het waarborgen van de staatsveiligheid en de openbare orde. Er zijn bepalingen opgenomen over het bevoegd aftappen en in verband met uitzonderlijke omstandigheden. Alle openbare telecommunicatienetwerken moeten zijn af te tappen.

Bij de Tw is toch een tweetal kanttekeningen op zijn plaats. De eerste betreft de onderscheidingen die in de Tw worden gehanteerd: openbaar/niet-openbaar, vast en mobiel, telecommunicatie en telefonie, omroepnetwerken, omroepzendernetwerken en telecommunicatienetwerken. Deze kunnen tot een snelle veroudering van de wet leiden. Immers, terwijl er sprake is van technische convergentie van communicatiemiddelen verbindt de wet verschillende rechtsplichten en/of -gevolgen aan mogelijk snel achterhaalde onderscheidingen.
Dit kan de ontwikkeling van nieuwe diensten – en nieuwe convergentie – remmen. Over enkele jaren moet nader worden onderzocht of de gehanteerde onderscheidingen ook in de toekomst nog steeds hanteerbaar zullen zijn. Zo nodig vindt dit onderzoek eerder plaats, in relatie tot het groenboek van de Europese Commissie over convergentie (zie daarvoor Deel II D van de nota).
De tweede kanttekening wordt geplaatst bij de regeling van het toezicht op de telecommunicatie- en mediasector. In augustus 1997 is de Onafhankelijke post- en telecommunicatieautoriteit (OPTA) in het leven geroepen, een onafhankelijke toezichthouder. De OPTA houdt toezicht op het gedrag van partijen op de telecommunicatiemarkt. Dit zou aanleiding kunnen geven tot afbakeningsproblemen met een andere toezichthouder op de markt, de NMA. Op het terrein van telecommunicatie en media is nog een derde toezichthouder actief, namelijk het Commissariaat voor de Media. Het Commissariaat heeft toezichtsbevoegdheden die betrekking hebben op de inhoudelijke aspecten van programmas die via telecommunicatienetwerken worden doorgegeven. Daarnaast is voor wat betreft de bescherming van de persoonlijke levenssfeer de Registratiekamer toezichthouder.

[1] Hierop is in onderdeel 3 van deze paragraaf ingegaan.

Dit levert allemaal nogal een verbrokkeld geheel op, waarbij het voor marktpartijen onduidelijk kan zijn tot welke toezichthouder zij zich moeten wenden. Een ander probleem van onduidelijke afbakening is de mogelijkheid tot forumshopping. In het MDW-rapport «Zicht op toezicht» worden op dit terrein voorstellen gedaan. Ook dit onderwerp moet over enkele jaren nader worden bezien.

4.7. Mededingingsrecht

4.7.1. Inleiding

Vrije mededinging staat hoog op de politieke agenda in de westerse wereld. In de jaren tachtig is in een aantal Europese landen de rol van de overheid bewust beperkt en is de wens uitgesproken overheidsdiensten te privatiseren en markten te dereguleren. Deze brede beweging in de richting van vrije markten is te zien op tal van niveaus. Op het niveau van de EU heeft allereerst de uitvoering van het Europese mededingingsbeleid door DG IV van de Europese Commissie meer prioriteit gekregen. Belangrijk is ook dat op Europees niveau is besloten tot liberalisering van een aantal markten die voorheen in handen van overheidsmonopolies waren, of in ieder geval zeer sterk gereguleerd waren. Te denken valt hier aan de transportmarkt, de telecommunicatiemarkt en de energiemarkt.

Veranderingen in mededingingsregimes zijn vooral ingegeven door het idee dat vrijhandel op mondiale schaal een groot goed is, waarvan de voordelen uiteindelijk alle burgers toekomen. Door internationaal belemmeringen weg te nemen, kunnen goederen en diensten vrijelijk worden verhandeld. Er ontstaan dan mondiale markten, waarop efficiënte allocatie mogelijk is en waardoor de prijzen lager worden.

Specifieke technologische invloed op veranderingen in mededingingswetgeving is overigens moeilijk aan te wijzen. Wel is technologie op een andere wijze van belang. Daar waar markten alleen kunnen functioneren door tussenkomst van technische middelen, moet worden vastgesteld in hoeverre de wens tot vrije mededinging niet wordt bemoeilijkt door technische factoren. Waar mogelijk kunnen dan aparte aanvullende regimes worden geschapen. Een voorbeeld hiervan is de nieuwe Telecommunicatiewet. Deze vult voor een deel de nieuwe Mededingingswet aan, waar deze laatste wet niet voorziet in de complicaties van de technisch complexe telecommunicatie-omgeving. Dergelijke aanvullende regels op gewone mededingingsregels zouden ook voor andere technologische markten en deelmarkten denkbaar zijn. Zie hiervoor Deel III E van deze nota.

4.7.2. Initiatieven op internationaal en Europees niveau

De afronding van de Uruguay-ronde van de GATT – General Agreement on Tariffs and Trade – en de daaruit voortgekomen oprichting van de WTO is een zeer belangrijke stap, die de openstelling van grenzen dichterbij brengt. De mogelijkheden die de technologie biedt om vanaf grote afstand handel te drijven en om productie in verschillende landen onder te brengen, lijken dan ook een passend internationaal handelskader te krijgen.
Op Europees gebied is er de afgelopen tien jaar in de structuur van het mededingingsregime, zoals die met name is vervat in de artikelen 85 en 86 van het EG-verdrag, geen principiële verandering geweest. Wel heeft de toepassing en handhaving van mededingingsregels door de Europese Commissie meer prioriteit gekregen. De Europese regelgeving is overigens wel van zeer groot belang geweest voor Nederland. De hieronder besproken nieuwe Mededingingswet beoogt expliciet Neder-

landse mededingingswetgeving in overeenstemming te brengen met de Europese wetgeving.

4.7.3. Betekenis voor Nederlandse wetgeving

a. De mededingswet
Het kabinet heeft duidelijke ideeën over de wijze waarop markten geordend moeten zijn. Vrije toetreding tot markten, vrije concurrentie en weinig belemmerende regels zijn algemene uitgangspunten voor marktwerking en -ordening. De voornaamste maatregel die het kabinet in de afgelopen regeerperiode heeft genomen om concurrentie te stimuleren, was de invoering van de nieuwe Mededingingswet per 1 januari 1998. De belangrijkste elementen van deze nieuwe wet zijn:

- de oprichting van de Nederlandse mededingingsautoriteit (NMA). Deze zal de controlerende activiteiten ter hand nemen, analoog aan DG IV van de Europese Commissie.
- een algemeen verbod op mededingingsbeperkende afspraken. Verboden worden: «besluiten en onderling afgestemde feitelijke gedragingen van ondernemingen die ertoe strekken ... dat mededinging wordt verhinderd, beperkt of vervalst». De oude Wet economische mededinging kende een misbruikstelsel: alleen de vanuit het gezichtspunt van het algemeen belang ongewenste excessen worden bestreden. De nieuwe wet hanteert een verbodsstelsel, met bovendien controle en handhaving vooraf. Met deze verandering is de wetsystematiek van de nieuwe wet in overeenstemming met die van de Europese regelgeving. De wet verbiedt zowel horizontale als verticale prijsbinding.
- verbod van misbruik van economische machtsposities.
- concentratieverbod. De NMA toetst, net als DG IV van de Europese Commissie, of fusies van grote ondernemingen – gezamenlijke omzet van de fusiepartners van meer dan 250 miljoen netto en tenminste twee partners met ieder een omzet van 30 miljoen in Nederland – of de nieuwe onderneming geen monopolie vormt of anderszins mededingingswetgeving schenden.
- bagatelvoorziening. Kleine ondernemingen en ondernemingen met een bijzondere taak kunnen een lichter mededingingsregime tegemoet zien.
- de mogelijkheid om boetes op te leggen. Deze geldstraffen bedragen maximaal 10% van de netto omzet.

b. Telecommunicatiewet
In de nieuwe Telecommunicatiewet – zie onder 6 – wordt een apart mededingingsregime voor de telecommunicatiesector ingesteld. De Memorie van Toelichting zegt hierover: «de noodzaak van deze specifieke regels vloeit (ook vanuit Europees kader) voort uit het feit dat de marktverhoudingen in delen van de telecommunicatiemarkt zo imperfect zijn dat het bereiken van een voldoende graad van mededinging te lang op zich zou laten wachten als uitsluitend het algemene mededingingsrecht zou worden toegepast. Daarom zijn specifieke regels opgenomen waaraan marktpartijen op voorhand moeten voldoen». De wet berust wat betreft het mededingingsregime op twee principes:

- Vrije toetreding: in principe is er vrije toetreding, er kunnen wel beperkingen gesteld worden op grond van schaarste-overwegingen, bijvoorbeeld in verband met de frequentietoedeling.
- Marktgedrag: voor partijen met een aanmerkelijke macht op de markt – meer dan 25% aandeel van een bepaalde markt – kunnen andere regels gelden dan voor kleinere partijen. Dit om te voorkomen dat dominante partijen ontstaan. Voorts zijn partijen verplicht tot interconnectie. Dat wil zeggen dat partijen van elkaars netwerken gebruik dienen te kunnen maken – en de netwerken dus technisch compatibel

moeten zijn – en dat de prijsstelling van wederzijds gebruik kostengeoriënteerd moet zijn. Partijen mogen dus niet worden geweerd door het berekenen van te hoge kosten.

Het toezicht op de telecommunicatiemarkt is opgedragen aan de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), die in het bijzonder zal toezien op de interconnectie. Mettertijd zal de OPTA opgaan in de NMA.

4.8. Fiscaliteit

4.8.1. Inleiding

De OESO is op fiscaal gebied het belangrijkste internationale forum. Aanvankelijk spitste de discussie over de invloed van de elektronische snelweg zich toe op de directe belastingen, maar sinds 1996 jaar worden ook de indirecte belastingen onderzocht.

4.8.2. Beïnvloeding door de elektronische snelweg

Twee aspecten van de elektronische snelweg hebben invloed op het fiscale stelsel: dematerialisering en internationalisering. Het feit dat veel handelingen niet aan plaats zijn gebonden en geschieden in een open, internationale samenleving bemoeilijkt mogelijk het heffen van belasting.

4.8.3. Initiatieven op internationaal niveau

In OESO-verband wordt thans een aantal studies verricht naar de invloed van de elektronische snelweg op zowel de directe als de indirecte belastingen. De volgende onderwerpen worden bestudeerd:

a. Directe belastingen

In het OESO-modelverdrag inzake de voorkoming van dubbele belasting, waarop de meeste Nederlandse belastingverdragen zijn gebaseerd, is het concept «vaste inrichting» opgenomen. Op grond van dit begrip worden de ondernemingsactiviteiten van niet-inwoners in de belastingheffing betrokken indien er sprake is van een vaste bedrijfsinrichting door middel waarvan de werkzaamheden geheel of gedeeltelijk worden uitgeoefend. Bij elektronische handel is het mogelijk dat de aanwezigheid van een dergelijke bedrijfsinrichting niet in alle gevallen even duidelijk is. De studie naar de gevolgen van elektronische handel voor het modelverdrag, zal begin 1998 leiden tot een eerste rapportage.

Er wordt steeds meer gedigitaliseerde informatie, zoals software, boeken, muziek, via de elektronische snelweg verkocht. De activiteiten van ondernemingen die vanuit Nederland worden uitgeoefend, worden in Nederland belast. Bij elektronische transacties zal het evenwel niet altijd duidelijk zijn waar deze plaats hebben. Ook de locatie van de leiding van een rechtspersoon is in een elektronische omgeving soms niet duidelijk omlijnd. In OESO-verband is een nadere studie over deze onderwerpen gewenst, waartoe door het kabinet initatief zal worden genomen.

De ontwikkelingen op het gebied van de elektronische snelweg leiden wat betreft de prijsstelling van transacties tussen gelieerde ondernemingen, «transfer pricing», niet tot nieuwe fundamentele problemen. Toch brengt de toename van elektronische handel de mogelijkheid met zich mee dat de «transfer pricing»-problematiek meegroeit. De traditionele aanpak bij «transfer pricing», zoals de beoordeling welke bedrijfsfuncties waar worden uitgevoerd, kan onder druk komen te staan. En dat geldt ook voor de vraag waar de daarmee samenhangende risico's thuishoren. Dit zal, als gevolg van steeds verder gaande elektronische integratie, waarschijnlijk

moeilijker worden bij internationale ondernemingen. De studie die hiernaar wordt verricht, zal naar verwachting begin 1998 tot rapportage leiden.
De beschikbaarheid van de informatie voor belastingadministraties kan mogelijk onder druk komen te staan als gevolg van cryptografie. Een aparte OESO-werkgroep – Cybertax Group – houdt zich bezig met de gevolgen van cryptografie. Er wordt onder meer gedacht aan Trusted Third Parties, die de encryptiesleutel onder bepaalde voorwaarden aan de overheid moeten verstrekken.

b. Indirecte belastingen
De OESO heeft onderzoek gedaan naar de invloed van de elektronische snelweg op het fiscale beleid met betrekking tot de verbruiksbelastingen. De belangrijkste conclusies hiervan zijn:
- De elektronische handel kan leiden tot een grotere hoeveelheid postordergoederen, waardoor de capaciteit van de controle onder druk kan komen te staan.
- Bij on-line transacties kan met de huidige omzetbelastingstelsels dubbele heffing en niet-heffing worden voorkomen.

Deze onderzoeksresultaten leiden tot de volgende beleidslijn:
Omzetbelastingen zijn algemene verbruiksbelastingen met een territoriaal karakter. Heffing dient plaats te hebben in het consumptieland en de belasting dient ten goede te komen aan de schatkist van dat land. Een belangrijk kenmerk van een dergelijke heffing is de neutraliteit op het gebied van de concurrentieverhoudingen. Dit uitgangspunt dient te worden verwezenlijkt door het voorkomen van niet-heffing – die leidt tot derving van belastingmiddelen in het consumptieland – en het voorkomen van dubbele heffing – die beïnvloedt de concurrentieverhoudingen.

Het voorkomen van niet-heffing en dubbele heffing van verbruiksbelasting kan worden bereikt door het treffen van de volgende maatregelen:
- De regels voor de plaats waar een prestatie wordt belast, «place of supply rules», dienen internationaal op elkaar te zijn afgestemd.
- De definitie van bepaalde prestaties dient uniform te zijn, omdat deze de toepassing van de regels voor de plaats van de prestatie beïnvloeden.
- De heffing kan worden verlegd naar de gebruiker, als eindgebruikers een administratie voeren. Dit is van belang als geen recht bestaat op aftrek van voorbelasting, zoals bijvoorbeeld bij banken en verzekeringsmaatschappijen.
- De controle moet worden afgestemd op de mogelijkheden die elektronische handel biedt: de zogeheten «audit trail». Te denken valt aan het volgen van betaalstromen.
- De mogelijkheden voor wederzijdse bijstand op het gebied van de indirecte belastingen moeten worden uitgebreid. Nederland heeft daartoe reeds besloten en zal internationaal de nodige stappen ondernemen.

4.8.4. Betekenis voor de Nederlandse wetgeving

Vooralsnog wordt niet overgegaan tot wijziging van de Nederlandse fiscale wetgeving. Daartoe worden eerst de resultaten afgewacht van de werkzaamheden van de OESO.

Als uitgangspunt voor regelgeving geldt voor het kabinet: handhaving van de concurrentieneutraliteit van het bestaande fiscale regime – onder andere door het voorkomen van dubbele heffing en dubbele vrijstelling. Daarnaast moet worden gewaakt voor derving van belastingmiddelen. Vooralsnog moeten de inspanningen erop zijn gericht dat doel met de bestaande heffingssystemen te realiseren. Mocht na verloop van tijd toch

aanpassing van het fiscale stelsel nodig blijken – bijvoorbeeld onder invloed van gewijzigde handelsstromen door elektronische handel – dan moet dit zoveel mogelijk gebeuren door middel van technologie-onafhankelijke wetgeving.

Tot slot heeft de Staatssecretaris van Financiën in december 1997 een adviesgroep geïnstalleerd, waarin de overheid en het bedrijfsleven samen de met elektronische handel samenhangende fiscale vraagstukken nader onderzoeken. De adviesgroep zal in het voorjaar van 1998 een advies uitbrengen.

4.9. Conclusies en voorstellen

- Artikel 7 van de Grondwet wordt aangepast aan de technologische ontwikkelingen, rekening houdend met nader onderbouwend onderzoek.
- Door middel van zelfregulering moet een classificatiesysteem voor mediaproducten tot stand komen, teneinde jeugdigen te beschermen tegen schadelijke invloeden van audiovisuele media. De overheid moet hierbij als subsidieverlener een stimulerende rol spelen.
- Het kabinet zal vervolg geven aan het Europese onderzoek naar mogelijkheden ter bevordering van de controle door ouders op kijkgedrag van minderjarigen.
- Maatregelen tegen geweld via audiovisuele middelen zijn alleen zinvol indien deze in Europees verband worden getroffen.
- Over enkele jaren bij de actualisering van de nota, moet nader worden bezien of:
  - de in de nieuwe Telecommunicatiewet gemaakte technische onderscheidingen, waaraan verschillende rechtsplichten en/of -gevolgen worden verbonden, ook in de toekomst hanteerbaar zijn.
  - Het toezicht op de telecommunicatie- en mediamarkt efficiënter kan worden geregeld. De voorstellen in het MDW-rapport «Zicht op toezicht» kunnen daarbij als leidraad dienen.
- Het kabinet zal het initiatief nemen om binnen OESO-verband een studie te laten verrichten naar de lokalisatie van elektronische transacties en de werkelijke leiding van rechtspersonen.
- Tot wijziging van Nederlandse fiscale wetgeving wordt pas overgegaan nadat over de regels en de voorschriften in internationale fora consensus bestaat.
- Bij eventuele wijziging van de Nederlandse fiscale wetgeving is technologie-onafhankelijke wetgeving het streven.

D. RECHTSVERGELIJKENDE ASPECTEN

1. Inleiding

Dit hoofdstuk bevat een overzicht van de belangrijkste juridische ontwikkelingen in Frankrijk, Duitsland, het Verenigd Koninkrijk en de Verenigde Staten met betrekking tot de elektronische snelweg. Waar nodig komen ook ontwikkelingen bij de Europese Unie aan de orde. Deze informatie is ontleend aan het onderzoek van Katholieke Universiteit Brabant «Netiquette of Wetiquette», dat in opdracht van het ministerie van Justitie is verricht en dat tegelijk met de nota wordt gepubliceerd[1]. Bij de beoordeling van de initiatieven tot regulering, dient rekening te worden gehouden met de specifieke verhoudingen en tradities in een land. Het onderzoek van de KUB is afgesloten op 1 oktober 1997.

2. Beleidsdocumenten

2.1. Europese Unie

De Europese Commissie heeft op 3 december 1997 een Groenboek over convergentie gepubliceerd.[2] De standpunten van de Commissie komen in grote mate overeen met de standpunten van de Amerikaanse regering (zie onder). In het Groenboek worden belemmeringen gesignaleerd, onder meer over:

- uiteenlopende voorwaarden voor de markttoetreding en vergunningen;
- onzekerheid over de in regelgeving gehanteerde concepten en over de wijze waarop bestaande regelgeving in de lidstaten wordt toegepast;
- problemen omtrent het vertrouwen van het publiek en het bedrijfsleven;
- meervoudig regelgevende instanties.

Evenals de Amerikaanse overheid lijkt de Europese Commissie een voorstander van een terughoudende overheidsrol. Waar regulering noodzakelijk is, staat de Commissie de volgende uitgangspunten voor:

- Regelgeving dient strikt noodzakelijk te zijn.
- Deze dient aan te sluiten bij de wensen van de gebruiker.
- Deze moet duurzaam en voorspelbaar zijn.
- Deze moet garanties bieden voor een universele participatie.
- Deze dient onafhankelijke en effectieve regelgevende instanties te creëren.

Met het Groenboek wordt op Europees niveau verder gebouwd aan een beleid, waarvan reeds uitgangspunten zijn te vinden in andere beleidsdocumenten, te beginnen met het rapport van de groep Bangemann uit 1994. Dit rapport schetst met name de werkzaamheden van de EU in verband met de elektronische snelweg. Het rapport wijst erop dat de EU het ontstaan van allerlei apart gereguleerde en gesubsidieerde deelmarkten moet tegengaan. Belangrijke doelstellingen zijn het versnellen van de marktwerking en het afbreken van monopolies in de Europese communicatiesectoren.
Andere recente beleidsdocumenten zijn het van april 1997 daterende document «Een Europees initiatief op het gebied van de elektronische handel»[3] en de in juli 1997 gepresenteerde «Verklaring van Bonn». Dit laatste document legt de nadruk op de overheidstaak om gunstige randvoorwaarden te scheppen. Wellicht dat het ingezette beleid in de toekomst resulteert in een European Communications Act. «Policy makers are having to come to terms with the realisation that they can rarely set the new rules of the game independently», aldus Europees Commissaris Bangemann.

[1] Ter inzage gelegd bij de afdeling Parlementaire Documentatie.
[2] COM (97) 623.
[3] COM(97)157 def.

2.2. Frankrijk

Verschillende initiatieven met betrekking tot Internet zijn stopgezet na het aantreden van de nieuwe regering in juni 1997. Dit heeft tot gevolg gehad, dat er op basis van eerdere beleidsrapporten nauwelijks praktische resultaten zijn te melden. Op 25 augustus 1997 heeft de Franse premier Jospin echter een actieplan van de Franse overheid aangekondigd. Een datum voor de publicatie van het actieplan werd daarbij niet genoemd.
De premier meent dat Internetgebruikers de verantwoording dragen voor het formuleren van gedragscodes voor afwijkend gedrag op Internet. Hij refereert hier aan vraagstukken rondom illegale en schadelijke informatie op Internet. Andere problemen dienen door de overheid op het meest geschikte niveau – dat wil zeggen: nationaal, Europees, of internationaal – te worden aangepakt. De Conseil d'Etat zal worden gevraagd om een studie te verrichten naar toekomstige keuzes ten aanzien van wet- en regelgeving voor Internet.
De Conseil d'Etat heeft drie commissies ingesteld en wel voor privacy, elektronische handel en auteursrecht. Deze commissies zullen waarschijnlijk in januari 1998 rapport uitbrengen.
Uit eerdere verschenen beleidsrapporten ontstaat omtrent regulering van Internet het volgende beeld:

- Bestaande wetgeving dient te worden aangepast.
- Zelfregulering heeft de voorkeur boven overheidsregulering.
- Nieuwe reguleringsactiviteiten moeten op internationaal niveau worden afgestemd, waarbij ook hier een voorkeur bestaat voor zelfregulering.
- Justitiële en politiële samenwerking tussen de EU-lidstaten wordt van groot belang geacht om naar een wereldwijde oplossing voor problemen op Internet toe te werken. De bevoegdheden onder de derde pijler van het EG-Verdrag zouden uitgebreid moeten worden, zodat ook Internet-criminaliteit hieronder valt.

Op 23 oktober 1996 heeft de Franse regering in de OESO een voorstel gedaan voor een «Charte de coopération internationale sur Internet» om het belang van internationale samenwerking te onderstrepen. De Charte stelt de volgende fundamentele kwesties aan de orde: het definiëren van gemeenschappelijke beginselen voor toepasselijk nationaal recht, het definiëren van de verantwoordelijkheden van Internet-actoren, de ontwikkeling van een gedragscode en het op gang brengen van politiële en justitiële samenwerking.

2.3. Duitsland

In het rapport «Info 2000: Deutschland's Weg in die Informationsgesellschaft» van februari 1996 geeft het Bondsministerie van Economie aan, dat internationale samenwerking en de ontwikkeling van een internationaal juridisch kader van groot belang. Dit vanwege het internationale karakter van ICT-netwerken. In dit verband wijst men op de ontwikkelingen ten aanzien van een Europese richtlijn voor strafrechtelijke aansprakelijkheid op Internet, welke op uitdrukkelijke wens van de Bondsregering is gestart. Het kabinet wil dat wetgeving op nationaal niveau wordt geünificeerd. Een direct uitvloeisel van dit beleidsvoornemen is de inmiddels aangenomen federale Wet op de informatie- en communicatiediensten («Gesetz zur Reglung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG)»), die als kaderwet een aantal zaken regelt.
Zowel de Bund als de Länder hebben wetgevingscompetentie op het gebied van informatie- en communicatiediensten. Op federaal niveau worden deze diensten bestreken door de wetgevingscompetentie met betrekking tot telecommunicatie. Op Länder-niveau worden deze diensten

door de wetgevingscompetentie die de Länder hebben met betrekking tot «Rundfunk». Het begrip Rundfunk wordt breed uitgelegd: het omvat alle diensten die op de openbaarheid zijn gericht, inclusief Internet-diensten.

2.4. Verenigd Koninkrijk

Het Verenigd Koninkrijk heeft tot op heden geen algemeen beleidsstuk voor een aanpak gepresenteerd. Hoewel het document al van eind 1996 dateert, moet «The House of Lords – Agenda for Action in the UK» daarom als belangrijkste beleidsdocument worden aangemerkt. Momenteel worden oplossingen veelal per sector of per onderwerp gezocht. Zo verscheen een document over elektronische handel, dat als «politiek belangrijk» wordt aangeduid. Wellicht dat de benadering onder de nieuwe regering zal veranderen. Hierover bestaat vooralsnog geen duidelijkheid. Een mogelijke indicatie voor de wijze van aanpak van de nieuwe Britse regering is het standpunt van Labour ten aanzien van de Information Superhighway. Het lijkt er echter op dat het aantreden van de nieuwe regering eerder een vertraging dan een versnelling in de ontwikkelingen betekent.

2.5. Verenigde Staten

In het rapport «A Framework For Global Electronic Commerce» van 1 juli 1997 opteert de Amerikaanse regering voor een non-regulatieve, op de markt georiënteerde benadering van de elektronische handel. Hierdoor wordt het ontstaan van een transparante en voorspelbare juridische omgeving bevorderd. Met het toenemende gebruik van het Internet ontstaat het gevaar dat overheden op grote schaal wet- en regelgeving met betrekking tot het Internet en de elektronische handel zullen gaan uitvaardigen. Deze kan de ontwikkeling van beide belemmeren. Dergelijke activiteiten moeten, volgens de Amerikaanse regering, worden gestopt voordat ze vaste vormen gaan aannemen.
De volgende uitgangspunten liggen ten grondslag aan de voorgestane benadering:

- De private sector vervult een voortrekkersrol. De overheid moet zelfregulering stimuleren. Bij Internet dient geen sprake te zijn van overheidsingrijpen, zoals dat is gebeurd bij telecommunicatie en de omroepen. Wel moet de overheid er voor zorgen dat er nationaal en regionaal geen barrières worden opgeworpen. Deze kunnen de toegang tot de nieuwe digitale markt belemmeren. Het bedrijfsleven moet zoveel mogelijk bij het beleidsproces worden betrokken als overheidsinterventie toch noodzakelijk is.
- Overheden moeten beperkingen voor de elektronische handel, zoals technologie-afhankelijke regelgeving, vermijden. Het inmiddels veelbesproken idee om van Internet een vrijhandelszone te maken, past hierin.
- Als overheidsinterventie nodig is, moet worden gestreefd naar een minimalistische, consistente, voorspelbare en eenvoudige juridische omgeving voor de elektronische handel.
- Overheden dienen de unieke kwaliteiten van Internet te erkennen. Dit betekent dat nieuwe wetgeving alleen moet worden uitgevaardigd bij belangrijke kwesties. Daarover moet tevens brede consensus bestaan.
- De elektronische handel moet op wereldwijde basis worden bevorderd. Het juridische raamwerk daartoe, moet bestaan uit beginselen die internationaal voorspelbare resultaten opleveren, ongeacht de jurisdictie waartoe partijen behoren.

3. Initiatieven tot regulering

3.1. Overheidsregulering

Duitsland heeft in de Wet op de informatie- en communicatiediensten als enige een algemene regeling opgesteld voor een groot aantal vraagstukken die zich voordeden als gevolg van de ontwikkeling van de elektronische snelweg. Deze wet is een kaderwet en voorziet in een regeling van:

- de aansprakelijkheid van Internetproviders;
- telediensten;
- de bescherming van persoonsgegevens bij elektronische diensten;
- de digitale handtekening (Gesetz zur digitalen Signatur, die verder is uitgewerkt in de Signaturverordnung) en
- gecertificeerde autoriteiten.

Een aantal onderwerpen geeft in verschillende landen aanleiding tot overheidsregulering of initiatieven daartoe. Het meest in het oog springend zijn:

- Illegale en schadelijke informatie op het Internet.
- Het creëren van een wettelijke basis voor «certification authorities» in verband met het gebruik van encryptie, waarbij de aanpak in de diverse landen overigens verschilt.
- Het creëren van goede toegang, waarbij mededingingsvrijheid, interconnectieverplichtingen en de rol van diversiteit van reguleringsautoriteiten, onderwerp van regulering zijn.
- Het reguleren van encryptie voor opsporingsdoeleinden. Alleen Frankrijk kent tot op heden een regeling. In Duitsland, het Verenigd Koninkrijk en de Verenigde Staten wordt hard gewerkt aan vergelijkbare voorstellen.
- Het aftappen van telecommunicatie in de elektronische omgeving leidt in de Verenigde Staten en Duitsland tot een herziening van de wettelijke regeling.
- Juridische betrouwbaarheid. De Verenigde Staten wijzen op de benadering van het Modelwet for Electronic Commerce van de UNCITRAL, waar het de juridische status van elektronische berichten en handtekeningen betreft.

3.2. Zelfregulering

Zelfregulering wordt in alle landen als een belangrijk instrument gezien. Wel geven de diverse overheden hier ieder een eigen invulling aan. In de Verenigde Staten spreekt men over zelfregulering als men zaken «echt» wil overlaten aan de markt. Dit impliceert dat er geen, of slechts een absoluut minimum aan kaderwetgeving wordt opgesteld. In Frankrijk noemt men zelfregulering als oplossing, maar men ziet daarbinnen voor de overheid toch een belangrijke sturende rol. Zelfregulering is in Duitsland belangrijk, maar de overheid wil toch invloed houden. Het Verenigd Koninkrijk zit tussen deze benaderingen in, waarbij de benadering meer lijkt op die in de Verenigde Staten, dan die in Frankrijk en Duitsland. Op de volgende terreinen wordt zelfregulering beoogd:

- Illegale en schadelijke informatie op Internet. Het Verenigd Koninkrijk ziet alleen bij schadelijke informatie een rol voor de betrokken partijen weggelegd. Illegale informatie is een zaak voor de rechter en de opsporings- en vervolgingsinstanties.
- Bescherming van persoonsgegevens. Initiatieven voor zelfregulering worden met name genomen in de Verenigde Staten en het Verenigd Koninkrijk.
- Juridische betrouwbaarheid. In de Verenigde Staten moet zelfregulering zorgen voor de gewenste juridische zekerheid.

- Technische aspecten van betrouwbaarheid. Standaarden moeten vanuit de markt worden ontwikkeld. In Duitsland wordt daarbij gewezen op de faciliterende en sturende rol van de overheid.
- Encryptie en Trusted Third Parties. Alleen de Verenigde Staten staan een aanpak voor vanuit de markt. In de VS is wetgeving voor digitale handtekeningen op het niveau van de staten afgekondigd.

4. Tot slot

Vanwege het internationale karakter van de elektronisch snelweg, kunnen de hierboven genoemde initiatieven tot nationale regulering veelal niet los worden gezien van internationale reguleringsinitiatieven en beleidsdocumenten. Voor een aantal onderwerpen wordt met name de beleidsontwikkeling op hoger niveau – Europees, internationaal – van groot belang geacht. Het één hoeft het ander overigens niet uit te sluiten. Het betreft de volgende onderwerpen:

- Illegale en schadelijke informatie. Aansturing vanuit de EU en de OESO vindt plaats. Deze aansturing wordt ook wenselijk geacht.
- Belasting. Aansturing vanuit internationaal niveau – onder meer OESO – wordt als wenselijk ervaren.
- Internationaal eenvormig privaatrecht. Met name vanuit de Verenigde Staten wordt op het belang van een internationale aanpak gewezen. Daarbij worden zowel de UNCITRAL, als de internationale Kamer van Koophandel genoemd.
- Bescherming van persoonsgegevens. De EU richtlijn 95/46/EG is bepalend.
- Juridische betrouwbaarheid. De Europese Commissie wil een kader geven voor betrouwbare communicatie in het algemeen en digitale handtekeningen in het bijzonder.
- Encryptie en Trusted Third Parties. Zowel de OESO, als, sinds kort, de Europese Commissie en de internationale Kamer van Koophandel hebben standpunten ingenomen. In de beleidsdocumenten van het Verenigd Koninkrijk, Frankrijk en Duitsland wordt gewezen op het belang van een internationale aanpak van dit onderwerp, waarbij de G7 en de EU als geschikte niveaus worden genoemd.
- Toegang en interconnectie. Het beleid dat door de EU op dit terrein wordt ontwikkeld, speelt een belangrijke aansturende rol.
- Auteursrecht en naburige rechten. Voor de Europese landen wordt het nationale beleid voornamelijk communautair gestuurd. De WIPO-verdragen leggen de verplichting op om wettelijke maatregelen te introduceren.

E. SYNTHESE

Uit de verschillende verkenningen blijkt dat:

- Al veel wetgeving in voorbereiding is – of zelfs al tot stand is gekomen – in reactie op de technologische ontwikkelingen. Hierbij valt te denken valt aan het voorontwerp voor een Wet Computercriminaliteit II, het nieuwe artikel 13 van de Grondwet, de Wet bescherming persoonsgegevens, de nieuwe Telecommunicatiewet en de liberalisatie van de Mediawet.
- Ook op Europees gebied en in andere internationale fora – bijvoorbeeld de OESO, voor fiscaliteit – actief wordt gewerkt aan het oplossen van de problemen waar de elektronische snelweg de wetgever voor stelt.
- Belangrijke delen van het Nederlands recht, waaronder de algemene delen van het privaatrecht en het strafrecht, technologie-onafhankelijk zijn en daardoor goed hanteerbaar voor de elektronische snelweg.
- Technologie-onafhankelijkheid niet altijd wenselijk is. Niet in alle gevallen kan van burgers worden verwacht, dat zij voldoende inzicht hebben om technieken op hun effectiviteit te beoordelen. Dit kan reden zijn voor technologie-afhankelijke regelgeving.
- Juridische constructies die zijn gebaseerd op technisch onderscheid, vaak hanteerbaar blijven door betere interpretatie, of door een nadere invulling van begrippen. Een goed voorbeeld hiervan is het lastig definieerbare verschil tussen transport en opslag van gegevens, dat echter wel op een juridisch zinnige wijze te hanteren is. Een dergelijke benadering kan ook bij andere problemen scherpe kanten van de elektronische snelweg wegnemen.
- De huidige uitgangspunten voor overheidsingrijpen – ordening op afstand, veel ruimte voor marktwerking, weinig productie door de overheid – ook voor de elektronische snelweg geschikt zijn.
- Technologische verandering niet zon effect heeft dat de structuur van het bestuur ingrijpende wijziging behoeft.
- De wijze waarop de overheid formeel met burgers communiceert, zoals vastgelegd in het bestuursrecht, aan de gewijzigde technologie kan worden aangepast.
- Technologische verandering voorlopig niet zo groot zal zijn, dat de burger alleen nog via de elektronische snelweg informatie zal kunnen krijgen, financiële transacties verrichten, of goederen aankopen.

Hiermee is het juridisch en bestuurlijk kader voor overheidsingrijpen in de informatiesamenleving echter niet af. Hoewel kan worden geconstateerd dat belangrijke stappen bij het overheidsoptreden op de elektronische snelweg nu reeds zijn gezet, blijven er nog belangrijke vragen over.
De elektronische snelweg kenmerkt zich door dematerialisering, internationalisering en technologische turbulentie. Dit beperkt de mogelijkheden van overheidsoptreden, zeker nu het kabinet als uitgangspunt heeft dat de elektronische omgeving geen onbestuurd of rechteloos gebied mag zijn. Ingrijpen zal dus niet nodig zijn om te zorgen dat algemene gewoonten en uitgangspunten ook op de elektronische snelweg gelden: wat «off-line» geldt moet ook «on-line» gelden.

De nota behandelt deze vragen verder aan de hand van vijf strategische themas, die uit de verkenningen worden afgeleid.

Deze thema's zijn:

1. Internationalisering en rechtsmacht
2. Privacy
3. Betrouwbaarheid
4. Markten
5. Rechtshandhaving

Bij de keuze van deze thema's is uiteraard ook gekeken naar de resultaten van het rechtsvergelijkend onderzoek: welke vragen staan in andere landen centraal?

De volgende nadere overwegingen moeten worden genoemd:

Ad 1 Internationalisering en rechtsmacht
Technologische ontwikkelingen en het wegvallen van handelsbelemmeringen leiden tot een sterke groei van jurisdictieproblemen. Wanneer burgers en bedrijven internationale contacten aanknopen en internationaal handel drijven, moet er ook een juridisch kader zijn waarop zij bij problemen kunnen terugvallen. Op dit moment is vaak niet duidelijk welk recht in welke gevallen geldt. Ook de betrekkingen tussen overheid en burger worden problematisch. Men kan hierbij denken aan het gesignaleerde probleem met de belastingheffing. Dit is het kernprobleem van de informatiesamenleving, dat de primaire overheidsfunctie raakt: het bieden van een juridisch en bestuurlijk kader. Een echte oplossing dient zich voor deze problemen nog niet aan. Aanzetten tot oplossingen hiervoor zullen worden behandeld bij het thema Internationalisering en rechtsmacht.

Ad 2 Privacy
De bescherming van de persoonlijke levenssfeer staat onder druk. Mensen begeven zich vaker – traceerbaar – op de elektronische snelweg. De mogelijkheden die de techniek biedt om gegevens op te slaan en te selecteren, zijn sterk vergroot. Voor de bescherming van persoonsgegevens zijn nieuwe wettelijke instrumenten in voorbereiding, zoals de Wet bescherming persoonsgegevens en de Telecommunicatiewet. Bij het thema privacy wordt gekeken of deze middelen de overheid en de burger voldoende uitrusten.

Ad 3 Betrouwbaarheid
De digitale techniek veroorzaakt de onmogelijkheid om onderscheid te maken tussen origineel en kopie. Waar de betekenis en waarde wordt toegekend aan het elektronisch signaal, neemt het belang van het onderscheiden van oorspronkelijke signaal en kopie sterk toe. Men denkt aan illegale CDs. Hoewel de techniek wel oplossingen biedt, is het van belang om het probleem van betrouwbaarheid en vertrouwen in een bredere dan alleen een technische context te benaderen. Technische oplossingen moeten immers worden ingebed in een juridisch en maatschappelijk kader. Daarbij kan het probleem van de betrouwbaarheid niet *alleen* vanuit de techniek worden behandeld. Bij het thema betrouwbaarheid zal vooral aandacht worden besteed aan de juridische, maatschappelijke en organisationele voorwaarden voor het scheppen van betrouwbaarheid op de elektronische snelweg.

Ad 4 Markten
De gelijktijdige verandering van mededingingsregime, telecommunicatiewetgeving en techniek maakt het nodig het functioneren van informatie- en telecommunicatiemarkten aan een nadere beschouwing te onderwerpen. Informatie is immers niet zomaar een «product», maar ook een essentiële voorwaarde voor politieke en maatschappelijke pluriformiteit. Dat blijkt bijvoorbeeld ook uit de nieuwe Telecommunicatiewet, waarin een afweging tussen maatschappelijke en economische belangen expliciet is opgenomen. Juist omdat informatie niet alleen «handelswaar» is, maar ook rechtsstatelijke – politieke pluriformiteit – en maatschappelijke – culturele pluriformiteit – functies vervult, is het van belang bij het thema markten te kijken naar de werking van informatiemarkten en naar de toegang tot die markten.

Ad 5 Rechtshandhaving

Handhaving is het sluitstuk van het recht. Veranderingen op het gebied van informatie- en communicatietechnologie hebben uiteraard ook effect op de rechtshandhaving. Voor het strafrecht is het relevant dat rond informatie- en communicatiesystemen nieuwe delicten ontstaan die het functioneren van informatiesystemen aantasten: «hacking», «bombing» en «spamming». Ook is van belang dat de elektronische snelweg voor traditionele delicten een nieuw medium is. Zo zijn bijvoorbeeld elektronische fraude en kinderporno via Internet nieuw. Daarnaast zal de techniek van opsporing en handhaving mee moeten groeien met de technische ontwikkeling.

De privaatrechtelijke handhaving verandert door de komst van de elektronische snelweg. Hierbij valt onder meer te denken aan de bewijsgaring en de komst van instellingen als TTPs, die ook handhavingsvragen oproepen.

Het thema rechtshandhaving gaat hierop in.

DEEL III STRATEGISCHE THEMA'S

A. INLEIDING

Dit deel van de nota bespreekt vijf thema's. Het thema internationalisering en rechtsmacht geeft een uitwerking van de meest fundamentele vraag die de informatiesamenleving oproept: hoe kunnen territoriaal georganiseerde overheden hun ordenende ambities waarmaken in een omgeving die zich van grenzen niets aantrekt?
De thema's privacy, betrouwbaarheid en markten zijn inhoudelijk van aard. Ze gaan in op de centrale beleidsdoelstellingen voor de bemoeienis van de overheid met de informatiesamenleving.
Het thema rechtshandhaving gaat in op de mogelijkheden om te komen tot het noodzakelijke sluitstuk van die bemoeienis, de handhaving.

Per thema wordt gekeken wat de ontwikkeling van informatiesamenleving betekent. De uitgangspunten van dit onderzoek komen voort uit eerdere delen van de nota. De belangrijkste:

- Drie aspecten van de elektronische snelweg vragen in het bijzonder om plaatsbepaling: dematerialisering, internationalisering en technologische turbulentie.
- Het niveau van ontwikkeling van de elektronische snelweg wordt gekenschetst als nevenschikkend. De nota biedt tevens oplossingen voor het niveau van ontwikkeling waarbij verdringing van traditionele communicatiemiddelen plaatsvindt.
- De overheid heeft op de elektronische snelweg een beperkte, ordenende taak. Wel is voor de overheid een faciliterende rol weggelegd bij de ontwikkeling van de informatiesamenleving.
- De normen die «off-line» gelden moeten ook «on-line» gelden.
- Waar traditionele middelen worden verdrongen, zal de overheid ook moeten zorgen voor toegankelijkheid.

Uit deel II komen voor het instrumentarium voorkeuren voort. In het algemeen bepaalt een terughoudende opstelling van de overheid de tendens:

- Technologie-onafhankelijkheid en globale normstelling maken regelgeving geschikt voor de elektronische omgeving.
- Zelfregulering wordt als belangrijk instrument gezien. Er is een voorkeur voor een internationale aanpak.

Er zijn echter ook trends in tegengestelde richting:

- Waar het gaat om de bescherming van grondrechten is een tendens te zien van regelverdichting.
- Soms vraagt de techniek zelfs om technologie-afhankelijke regelgeving.
- Dit geldt in het bijzonder waar de overheid het elektronisch rechtsverkeer wil bevorderen.

B. INTERNATIONALISERING EN RECHTSMACHT

1. Inleiding

De informatiesamenleving is vooral een open samenleving. Digitaal verwerkte informatie kan hierdoor niet alleen tot in de verste uithoeken van een samenleving doordringen, maar ook vrijelijk over de wereld reizen. Bij elektronische betrekkingen hebben fysieke afstanden en staatkundige grenzen daarom veel minder betekenis dan bij «gewone» betrekkingen. Dat speelt in het bijzonder bij Internet. De plaats waar een burger of instelling zich fysiek bevindt, hoeft niet de plaats te zijn waar deze activiteiten ontplooit. De gevolgen van die activiteiten beperken zich al helemaal niet tot de plaats waar de betrokkene zich bevindt. Om het nog ingewikkelder te maken: het is zelfs niet altijd vast te stellen waar activiteiten plaats hebben.
Deze internationalisering van informatiestromen en rechtshandelingen stelt overheden voor steeds grotere problemen. Zij hebben nu eenmaal in beginsel een rechtsmacht die aan een specifiek territoir is gebonden. Zij worden geconfronteerd met activiteiten die binnen hun landsgrenzen effect hebben – bijvoorbeeld bij verspreiding van informatie, verkoop van goederen of diensten, of het ontstaan van inkomsten waarover belasting geheven zou moeten worden – maar die worden verricht door personen die zich buiten hun territoir bevinden.
Anderzijds stelt deze internationalisering ook burgers en bedrijven voor de nodige problemen. Een groot aantal landen kan rechtsmacht claimen over dezelfde activiteiten, omdat al die landen effecten van die activiteiten ondervinden. Het beste voorbeeld hiervan is Internet: informatie die op een web-site of nieuwsgroep wordt aangeboden, is in beginsel in de gehele wereld opvraagbaar en zou daarmee onder een groot aantal rechtsstelsels vallen. Het thema Internationalisering en rechtsmacht speelt daarom een centrale rol in deze nota. Veel vragen over de rol van de overheid in een elektronische omgeving zijn terug te voeren op de spanning tussen de territoriale organisatie van de overheid aan de ene kant en het internationale karakter van elektronische handelingen aan de andere kant.[1]

De overgang van een traditioneel juridisch speelveld – daarbij is nationale soevereiniteit de kern – naar een dematerieel en internationaal speelveld, leidt voor de wetgever in de eerste plaats tot vragen over opeenstapeling van rechtsmacht en over de mogelijkheid en wenselijkheid van materieelrechtelijke, inhoudelijke harmonisatie.
Uitgangspunt daarbij: in veel gevallen is de Nederlandse wetgeving van toepassing op activiteiten die buiten Nederland worden verricht. Zelfs het territorialiteitsbeginsel beperkt de werking van het Nederlandse strafrecht niet tot die handelingen die in Nederland worden verricht. Ook handelingen waarvan zich het gevolg in Nederland voordoet, vallen onder het Nederlandse strafrecht. De komst van de elektronische snelweg roept echter een drietal kwesties op, die specifieke aandacht van de wetgever vragen:

- De opeenstapeling van rechtsmachten.
- De handhaving van nationale wetgeving.
- Het tekort schieten van de rechtsmacht.

Aan het slot van deze inleiding is een relativering op zijn plaats. Zoals in Deel II C naar voren is gekomen, ziet veel wetgeving op handelingen die naar hun aard niet grensoverschrijdend plaatsvinden. Het gaat dan om handelingen die ofwel aan plaats zijn gebonden – ruimtelijk bestuursrecht, bouwvoorschriften, grote delen van de sociale zekerheid – ofwel om handelingen die voor een burger of onderneming zo ingrijpend zijn, dat men niet met een elektronische transactie wenst te volstaan; men wil zijn

[1] Ten behoeve van de onderbouwing van deze nota heeft het Programmabureau Informatietechnologie en Recht een drietal workshops georganiseerd, met als titel «Regulering van het Internet». Tijdens deze workshops hebben deskundigen gediskussieerd over de vragen die het thema Internationalisering en rechtsmacht oproept. De uitkomsten van deze workshops vormden een belangrijke inspiratiebron voor dit hoofdstuk. Het verslag van deze workshops is gepubliceerd in deel 9 van de ITeR-reeks.

wederpartij «zien». Niettemin vormt internationalisering hét grote probleem.

2. Opeenstapeling van rechtsmachten

2.1. Algemeen

Dit probleem hangt samen met een specifieke eigenschap van Internet: op dit moment is het technisch niet goed mogelijk Internet geografisch te compartimenteren. Dit betekent dat een burger of rechtspersoon die informatie op Internet zet, of een «open» commerciële aanbieding doet, er rekening mee moet houden dat die informatie waar ook ter wereld is op te vragen en zodoende binnen de rechtsmacht van een reeks van landen kan vallen.[1] Zo bepalen enkele Europese ipr-verdragen – EEX en EVEX – dat er rechtsmacht bestaat in geval van een onrechtmatige daad:

- Ter plaatse van de woon- c.q. vestigingsplaats van de gedaagde.
- Ter plaatse waar het schadebrengende feit zich heeft voorgedaan.
- In een internationaal geval op de plaats waar de schadebrengende handeling is verricht en tevens op de plaats waar deze handeling zijn uitwerking heeft.

Bij een onrechtmatige daad via Internet is dus niet alleen de rechter in het land van vestiging van de gedaagde bevoegd, maar ook de rechters van de plaatsen waar het schadebrengende bericht wordt gelezen of waar bijvoorbeeld een schadebrengende virus zijn vernietiging heeft verricht. Doordat, naast Nederland, ook een reeks van andere landen rechtsmacht kan claimen over uitingen die via Internet worden verspreid, doet zich al snel een opeenstapeling van rechtsmachten voor. Burgers en bedrijven lopen daarmee het risico van meervoudige aansprakelijkheid: een bepaalde handeling of uiting kan in verschillende landen leiden tot civiele of strafrechtelijke aansprakelijkheid. Dit belemmert niet alleen de werking van Internet als forum voor meningsuiting, maar kan ook een belangrijk obstakel zijn voor de verdere ontwikkeling van de elektronische handel. Deze opeenstapeling van rechtsmachten leidt immers tot een grote mate van rechtsonzekerheid. Voor burgers en bedrijven is het onmogelijk om het recht van alle op Internet aangesloten landen te kennen en dus om de juridische risicos in te schatten.
Overheden en rechters in het bijzonder, worden bovendien geconfronteerd met de extraterritoriale werking van gerechtelijke uitspraken. Dit speelt vooral bij vorderingen in geval van onrechtmatige uitingen of bij inbreuken op intellectuele eigendomsrechten via Internet. Vorderingen die worden toegewezen hebben effect op andere rechtsstelsels, doordat zij die andere rechtsstelsels een rechtsverhouding opleggen. Deze rechtsverhouding kan strijdig zijn met het materiële recht dat ter plaatse wordt gehanteerd[2].

Indien verschillende landen ten aanzien van één handeling op de elektronische snelweg rechtsmacht claimen of uitoefenen, doen zich vragen voor van verschillende aard:

- Hoe kan de burger weten welke rechtsstelsels op hem van toepassing zijn en aan welke normen hij zich moet houden?
- Hoe kan worden voorkomen dat een burger voor dezelfde handeling in verschillende landen wordt vervolgd?
- Hoe kan worden voorkomen dat nationale rechters hun recht aan andere rechtsstelsels opleggen? Voor deze vraagstukken zijn verschillende oplossingen denkbaar.

2.2. Internationale harmonisatie

Internationale harmonisatie van materiële normen zou een belangrijk deel van de problemen rond de opeenstapeling van rechtsmachten en de

[1] Wij gaan er op dit moment vanuit dat het voor rechtssubjecten vooralsnog onmogelijk is om Internet langs territoriale lijnen te compartimenteren. Indien zij uitingen op Internet plegen zijn deze in beginsel waar ook ter wereld raadpleegbaar. Anders: G. Wierda, 1996 .
[2] Dit inzicht is ontleend aan de bijdrage van C.E. Drion, blz. 145 Regulering van het Internet.

daaruit voortvloeiende rechtsonzekerheid kunnen voorkomen. Op zichzelf gaat van de internationalisering van de samenleving reeds een harmoniserende werking uit. De wereld wordt kleiner en culturen komen dichter bij elkaar. De overheid zou daarnaast internationale harmonisatie ook actief kunnen bevorderen, bijvoorbeeld door middel van internationale afspraken. Deze weg is echter niet altijd begaanbaar of aantrekkelijk.
In de eerste plaats kiest het kabinet als uitgangspunt dat de normen die gelden voor de elektronische snelweg hetzelfde dienen te zijn als de normen in de fysieke wereld. De inhoudelijke argumenten om in de fysieke wereld een bepaald rechtsterrein niet, in beperkte mate, of juist wel te harmoniseren, zoals grote delen van het economisch ordeningsrecht, spelen ook hier een doorslaggevende rol. In die zin biedt de elektronische snelweg niets nieuws.

In dit verband verdient het commune strafrecht aparte vermelding, omdat hieraan vaak fundamentele culturele normen en waarden over eerbaarheid van gedragingen ten grondslag liggen. In Nederland wijken deze op bepaalde terreinen af van die van de meeste grote westerse landen. Harmonisatie betekent daarmee in feite een eenzijdige aanpassing van het Nederlands strafrecht. Ook buiten het strafrecht moet rekening worden gehouden met het wereldwijde karakter van vele onderdelen van de elektronische snelweg en daardoor met het wijd uiteenlopen van normen en waarden. Bovendien kan het vervolgens voor individuele landen aantrekkelijk zijn om zich aan harmonisatie te onttrekken, bijvoorbeeld bij het instellen van gok- of belastingvrijhavens.

Resumerend: internationale harmonisatie van materiële normen moet worden nagestreefd waar dit kansrijk is. Daarbij kan men met name denken aan:
- economische ordening,
- privaatrecht,
- vermogensdelicten,
- specifieke computerdelicten, zoals hacking,
- vergrijpen waarover een brede internationale consensus bestaat, zoals kinderporno en extreem geweld en
- onderwerpen waarover internationaal erkende gemeenschappelijke inzichten bestaan, zoals die welke zijn neergelegd in het BUPO-Verdrag en in andere VN-Verdragen.

Deze internationale harmonisatie vergt een gecoördineerde aanpak van een reeks voorstellen. Op dit punt zal het kabinet daarom nauw aansluiting zoeken bij de gedachten die leven bij de Europese Commissie om te komen tot een Europese afstemming van de wetgevingsagenda rond de elektronische snelweg. Daarbij dient men zich echter te realiseren dat internationale harmonisatie soms aanpassing van Nederlandse materiële normen vergt aan de internationale consensus. Het kabinet wijst zo'n aanpassing niet op voorhand af. Verder is internationale harmonisatie een zaak van de lange adem.

2.3. Vrijhavens

Het ontstaan van vrijhavens zal op de elektronische snelweg nooit geheel kunnen worden vermeden. Er zullen altijd landen zijn die zich onttrekken aan internationale regels, zowel waar het gaat om materiële regels, als om regels over rechtshandhaving. Het kan dus aantrekkelijk zijn om informatie vanuit die landen op de elektronische snelweg aan te bieden. Aan de andere kant kan, als er brede internationale consensus bestaat, de effectiviteit van die vrijhavens op een aantal manieren worden beperkt:
- Met name voor commerciële transacties zullen vrijhavens niet aantrekkelijk zijn. Bij het publiek zal in dergelijke landen niet veel vertrouwen bestaan.

- Een nadere regeling van de aansprakelijkheid van tussenpersonen kan een oplossing bieden – zie hieronder.
- Via economische sancties – onder meer in het verband van de WTO - kunnen landen die een bedreiging vormen voor de mondiale rechtsorde, worden gedwongen hun status van vrijhaven op te geven. Dit middel is erg zwaar en alleen geschikt bij flagrante schendingen van de mondiale rechtsorde. Wellicht bieden WTO-geschillenpanels betere mogelijkheden.

Concluderend: het bestaan van vrijhavens is onvermijdelijk, maar hun reikwijdte kan aanzienlijk worden beperkt. Internationale afspraken zijn hiertoe geboden.

2.4. Reikwijdte strafrechtsmacht

Bij de behandeling van de Justitiebegroting van 1997 is de Minister van Justitie uitgegaan van een beperkte opvatting van de rechtsmacht ten aanzien van uitings- en verspreidingsdelicten via de elektronische snelweg. De Nederlandse rechtsmacht wordt in ieder geval uitgeoefend ten aanzien van uitingen die naar woord en inhoud op Nederland zijn gericht[1]. In andere gevallen zal uitoefening van rechtsmacht minder prioriteit hebben. Het is gewenst deze uitgangspunten ook in internationale afspraken neer te leggen. Indien dit niet haalbaar is, zou men kunnen streven naar internationale afspraken tussen landen over onderlinge prioritering bij de uitoefening van rechtsmacht. Reeds in 1990 is in het kader van de Raad van Europa een studie naar dit onderwerp gedaan. Het bleek toen echter niet mogelijk om tot afspraken te komen[2]. Voor deze problematiek dient, naar analogie van de aanknopingsleer van het internationaal privaatrecht, een oplossing te worden gezocht. Aanknopingspunten kunnen zijn: verblijfplaats, nationaliteit, land waar gedraging zich op richt, of het land waar zich daadwerkelijk effecten voordoen,

2.5. Internationaal privaatrecht

In deel II C-1 wordt uiteengezet dat het huidige internationaal privaatrecht slechts in beperkte mate geschikt is om ook op Internet-conflicten te worden toegepast. Er zijn soms meer rechtsstelsels tegelijk van toepassing. Hierdoor zal op voorhand onduidelijk zijn welk nationaal recht op een bepaalde rechtsverhouding van toepassing is. Slechts in de Verenigde Staten is ook aandacht voor deze specifieke problematiek, die zich overigens concentreert op elektronische handel. Gelet op het mondiale karakter van Internet zijn de Verenigde Staten dan ook een sterk voorstander van het ontwikkelen van een wereldwijd commercieel juridisch kader, dat partijen door middel van een rechtskeuze op hun overeenkomsten van toepassing kunnen verklaren. Dit teneinde problemen over rechtsmacht te vermijden. Bij het opstellen van een dergelijk juridisch kader stellen de Verenigde Staten zich op het standpunt dat hier, alhoewel overheidsinterventie met het oog op de ontwikkeling van adequate en doelmatige mechanismen voor de oplossing van conflicten noodzakelijk is, zelfregulering door de deelnemers aan de elektronische handel een belangrijke plaats dient in te nemen. Verder sporen de Verenigde Staten internationale organisaties, zoals UNCITRAL, UNIDROIT en de internationale Kamer van Koophandel aan om internationale beginselen voor de elektronische handel te definiëren.
Het kabinet onderkent het belang van het opstellen van internationale privaatrechtelijke regels voor elektronische handel. Het kabinet zal dan ook de initiatieven van de Verenigde Staten ondersteunen. Dit betekent dat ook Nederland de genoemde internationale organisaties zal stimuleren om internationale privaatrechtelijke beginselen voor elektronische handel op te stellen en zelf een actieve inbreng te leveren. Het is daarbij

[1] Het ging daarbij in concreto om een vanuit de VS op Internet gezette racistische uitlalting, die in het Nederlands was gesteld en was gericht op omstandigheden in Nederland, IIK Handelingen 1996–1997, nr 29, p. 2342–2345.
[2] Extraterritorial criminal jurisdiction: report of the Council of Europe.

van belang om daarin ook de deelnemers aan elektronische handel te betrekken. Daarnaast zal het kabinet hoge prioriteit geven aan het opstellen van een bredere Internet-ipr-regeling in het kader van de Haagse Conferentie (zie Deel II C-1 van de nota).

3. Handhaving van nationale wetgeving

Een tweede vraag met betrekking tot internationalisering is: hoe kan het recht worden gehandhaafd jegens individuen die zich fysiek buiten de Nederlandse jurisdictie bevinden, maar handelingen verrichten met gevolgen binnen die jurisdictie. De effectiviteit van de Nederlandse wetgeving komt ook onder druk te staan wanneer het omgekeerde gebeurt. Hierbij kan worden gedacht aan het in andere landen aanhouden van spaartegoeden, het deelnemen aan gokactiviteiten, het kopen van geneesmiddelen zonder recept of het kopen van wapens.
Deze paragraaf beperkt zich tot handhavingsvraagstukken die een rechtstreekse relatie hebben met de rechtsmacht van staten: hoe kan het recht worden gehandhaafd jegens individuen die zich fysiek buiten onze jurisdictie bevinden, maar handelingen verrichten met gevolgen binnen die jurisdictie?

3.1. Handhaving van het strafrecht

3.1.1. Internationale samenwerking

Het strafrecht voorziet voor handhaving ten aanzien van verdachten die zich buiten Nederland bevinden in een aantal instrumenten, onder meer in de vorm van een groot aantal bilaterale rechtshulpverdragen. Daarnaast worden de strafvorderlijke mogelijkheden vergroot via de samenwerking in de Raad van Europa en de derde pijler van de Europese Unie op het gebied van de interceptie van Internet-, respectievelijk satellietcommunicatie. Teneinde een effectieve handhaving te bereiken, is een goede samenwerking tussen opsporingsautoriteiten vereist. De snelheid van informatie-uitwisseling in de elektronische omgeving vergt ook een snelle reactie. Zo blijkt uit de evaluatie van het Internet Meldpunt Kinderporno, dat de traagheid in de samenwerking tussen autoriteiten de opsporing nog wel eens belemmert.
Verbetering van de strafrechtelijke handhaving kan worden bereikt door deze bestaande instrumenten optimaal te benutten en daarnaast de instrumenten zelf op onderdelen aan te passen. Dat laatste is in het bijzonder nodig om:

- de opsporingsbevoegdheden jegens buitenlandse providers te reguleren en
- medewerking van andere landen bij de opsporing te verzekeren.

Binnen de deskundigengroep «Crime in cyberspace» van de Raad van Europa worden daartoe voorstellen ontwikkeld, die moeten leiden tot een verdrag van de Raad van Europa. In dit verdrag dient in ieder geval prioriteit te worden gelegd bij de mogelijkheden om onmiddellijk informatie te verkrijgen van providers die zich in andere landen bevinden. Dit om te voorkomen dat sporen verloren gaan. De noodzakelijke rechterlijke toetsing dient dan achteraf plaats te vinden.

3.1.2. Het vereiste van dubbele strafbaarheid

Een drempel voor de handhaving van het strafrecht in de elektronische omgeving en het maken van internationale rechtshulpafspraken daarover, wordt gevormd door het vereiste van dubbele strafbaarheid. Aan de strafrechtelijke handhaving in een ander land wordt alleen meegewerkt indien de betreffende handeling ook in het eigen land strafbaar is.

Hierdoor wordt het aantrekkelijk om een delict in land X te plegen vanuit land Y, waar de betreffende handeling niet strafbaar is.
Onder voorwaarden zou het mogelijk moeten zijn af te wijken van het vereiste van dubbele strafbaarheid. In de eerder genoemde deskundigengroep van de Raad van Europa «Crime in Cyberspace» stellen de Verenigde Staten (als waarnemer aanwezig) voor om het vereiste los te laten ten behoeve van het inwinnen van inlichtingen teneinde het elektronische spoor te kunnen reconstrueren. Het Europees rechtshulpverdrag[1] vormt op zichzelf geen belemmering en staat toe af te wijken van de eis van dubbele strafbaarheid. Nederland heeft destijds een voorbehoud gemaakt bij die afwijkingsmogelijkheid. Dit voorbehoud kan ten behoeve van de handhaving van het strafrecht in de elektronische omgeving komen te vervallen, mits er:

- geen sprake is van uitlevering. De rechtshulp zal alleen zien op informatieverschaffing, teneinde het elektronische spoor te kunnen reconstrueren.
- wordt voldaan aan enkele andere voorwaarden, zoals: afspraken op basis van reprociteit, alleen rechtshulp bij van te voren bepaalde ernstige delicten, het delict zal moeten zijn gericht op de rechtsorde van het land dat om rechtshulp verzoekt, notificatie achteraf aan de betrokken persoon.

Het maken van dergelijke afspraken moet uiteraard worden bezien in samenhang met de hierboven genoemde maatregelen over de samenwerking van autoriteiten.

3.2. Handhaving van het bestuursrecht

In Deel II C-2 wordt uitgebreid ingegaan op de handhavingsproblematiek van het bestuursrecht op de elektronische snelweg. Oplossingen worden gezocht in aanpassing van het Nederlands recht:

- bij ernstige overtredingen van bestuursrechtelijke normen die vanwege de betrokken Nederlandse belangen een grote inbreuk op de rechtsorde opleveren zullen deze belangen in een strafbaarstelling tot uiting moeten komen.
- het kabinet stelt voor de reikwijdte van het regime van vergunningenstelsels uit te breiden naar buitenlandse dienstenaanbieders die op de Nederlandse markt opereren.

De problematiek van handhaving van het bestuursrecht leidt niet tot voorstellen gericht op het totstandbrengen van internationale maatregelen. Wat hierboven over het strafrecht wordt gesteld geldt mutatis mutandis voor het bestuursrecht.

3.3. Handhaving van het privaatrecht

Ook in het privaatrecht geldt het uitgangspunt dat altijd een verantwoordelijke moet zijn aan te wijzen voor onrechtmatige handelingen op de elektronische snelweg (zie Deel II C-1). Het leerstuk van de onrechtmatige daad biedt vooralsnog voldoende houvast om in voorkomende gevallen de tussenpersoon onrechtmatige daden toe te rekenen. Dit leerstuk biedt echter alleen een oplossing als het tussenpersonen betreft die in Nederland zijn gevestigd. De volgende vraagstukken resteren:

- Als de onrechtmatige handeling niet door een nationale tussenpersoon wordt doorgegeven, hoe kan dan worden achterhaald waar de handeling wordt verricht, of door welke tussenpersoon de handeling wordt doorgegeven?
- Kan een Nederlandse burger ook een buitenlandse tussenpersoon aansprakelijk stellen voor onrechtmatige handelingen, die door deze provider worden doorgegeven?

[1] Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken.

Net als voor de opsporingsautoriteiten is het dus ook voor de burger van belang om een elektronisch spoor te kunnen reconstrueren, teneinde zijn recht te kunnen handhaven. Daarvoor zal veelal de medewerking van tussenpersonen vereist zijn. Voorts is het afhankelijk van het nationale recht van het land waarin de tussenpersoon zich bevindt of, wanneer de identiteit van de schadeveroorzakende partij onbekend is, de tussenpersoon voor de onrechtmatige handeling aansprakelijk kan worden gesteld. De privaatrechtelijke aansprakelijkheid van tussenpersonen en het kunnen nagaan van het elektronisch spoor door de burger vormen thans in internationale fora evenwel nog geen punt van aandacht. Het kabinet zal internationale organisaties, zoals de Raad van Europa, aansporen voorstellen te doen over privaatrechtelijke aansprakelijkheid van tussenpersonen. Dit om tot een uniforme regeling te komen. Daarbij dient het eerder geformuleerde uitgangspunt te worden gehanteerd, dat voor onrechtmatige handelingen in een elektronische omgeving altijd een verantwoordelijke moet zijn aan te wijzen. Het door de burger kunnen traceren van het elektronisch spoor met medewerking van tussenpersonen, zal eveneens onder de aandacht van internationale organisaties worden gebracht. Daarbij moet in gedachten worden gehouden dat de medewerking van tussenpersonen tot een botsing kan leiden met andere aan burgers toegekende rechten, zoals het recht op privacy.

4. Tekort schieten van de rechtsmacht

De Nederlandse rechtsmacht schiet tekort op het moment dat van buiten de Nederlandse rechtssfeer handelingen worden verricht die de Nederlandse rechtsorde raken, maar waarvoor het Nederlands recht geen aanknopingspunt voor rechtsmacht biedt. Dit is in eerste instantie een probleem voor de nationale wetgever. Het wordt met name veroorzaakt door het feit dat de elektronische snelweg het veel makkelijker maakt om handelingen naar het buitenland te verplaatsen, terwijl het recht nog steeds uitgaat van fysieke aanwezigheid binnen het territorium van de Nederlandse staat. Aanpassing van de nationale wetgeving kan in deze gevallen geboden zijn.
Naar het zich thans laat aanzien, doet dit probleem zich maar in een beperkt aantal gevallen voor. Zo is voor de belastingheffing vaak een fysiek aangrijpingspunt in Nederland nodig, terwijl in een elektronische omgeving de betreffende handeling of betaling eenvoudig naar het buitenland is te verplaatsen. Daarbij is het bovendien niet altijd eenvoudig de plaats van de elektronische handeling te bepalen. Soortgelijke problemen ziet men in de sfeer van de telecommunicatie, de sociale wetgeving en het bestuursrecht. Het niet meer hanteerbare fysieke aangrijpingspunt zal in dergelijke gevallen moeten worden vervangen, of in ieder geval aangevuld met een ander aangrijpingspunt. Indien deze zich in Nederland bevindt, is bijvoorbeeld de plaats van de tussenpersoon daarvoor geschikt. Ook de plaats van de infrastructuur behoort tot de mogelijkheden. Bij mobiele communicatie via satellieten is echter ook die laatste oplossing niet geschikt. In die gevallen zal een ander aangrijpingspunt in Nederland moeten worden gecreëerd, bijvoorbeeld rechtstreeks bij de consument[1].

5. Nadere uitwerking van de oplossingsrichtingen

5.1. Supranationale regelgeving is gewenst

Vanwege het internationale karakter van deze problematiek vindt regelgeving bij voorkeur plaats op een hoog niveau. Mondiale verdragen zijn het meest geschikt; zij zullen echter niet in alle gevallen haalbaar zijn. Dit vanwege de te zeer uiteenlopende opvattingen over het recht en de diversiteit aan normen en waarden die daarin zijn neergelegd. Waar met

[1] Ontwerp-overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lid-staten van de Europese Unie, art. 8.

name het elektronisch verkeer tussen westerse landen regulering behoeft, zijn ook de Raad van Europa en de OESO geschikte fora. Opgemerkt zij overigens dat in de Raad van Europa-groepen over criminaliteit en Internet de Verenigde Staten en Canada nu al een actieve rol spelen. Soms zal het EU-niveau een aanvaardbare «second-best»-oplossing bieden.
Een keuze voor nationale wetgeving kan gerechtvaardigd zijn:
- ter bescherming van normen en waarden,
- indien regelgeving op internationaal niveau niet haalbaar is, of te lang zou duren,
- om de concurrentiepositie van Nederland te versterken, of
- als voorbeeldfunctie voor de internationale rechtsontwikkeling.

Wanneer regulering om inhoudelijke redenen gewenst is, mag een gebrekkige haalbaarheid van internationale regelgeving echter nooit een reden zijn om toch maar van regelgeving af te zien.

5.2. Internet als eigensoortig rechtsgebied

Vanwege het bijzondere karakter van Internet, zou men kunnen kiezen voor een specifieke wet of een speciaal verdrag over Internet: een «Lex Internet». Zo'n Lex Internet zou het «gewone recht» kunnen aanvullen, of op onderdelen vervangen. Het specifieke, principieel internationale karakter van Internet kan namelijk meebrengen dat bestaande rechtsstructuren, uitgaande van de soevereiniteit van territoriale staten, onvoldoende soelaas bieden. Net zoals voor het zeerecht specifieke regels zijn ontwikkeld, zou dit voor Internet kunnen geschieden. Mogelijke onderwerpen van zo'n Lex Internet zouden kunnen zijn:
- Codificatie van gedragsnormen op de elektronische snelweg[1].
- Illegale inhoud van uitingen.
- Extreem geweld.
- Privacy en bescherming van data.
- Computercriminaliteit.
- Vrijheid van meningsuiting en censuur.
- Elektronische handel.
- Toekennen van domeinnamen.
- De verplichting de toegekende domeinnamen te gebruiken.

Tezamen met onder andere de Raad van Europa en de Europese Commissie vindt op dit moment een gedachtewisseling plaats over de mogelijkheden van specifieke regelgeving voor Internet op nationaal of op internationaal niveau. Een Lex Internet, in de zin van een specifiek verdrag, staat daarbij niet op de agenda. Internationale oplossingen worden daarvoor niet haalbaar geacht. Zoals ook bij de Conferentie «Global Information Networks» in Bonn bleek, gaat men er vooralsnog vanuit dat wat geldt in de fysieke wereld gelijkelijk moet gelden in de elektronische omgeving. Dat betekent dat een aparte wet met aparte normen voor Internet niet gewenst is. Het kabinet stelt zich eveneens op dit standpunt. Er is echter nog een tweede reden waarom op dit moment een Lex Internet niet opportuun is: de technologische turbulentie. Thans valt niet goed te voorspellen in welke richting Internet, of een opvolger daarvan, zich de komende jaren zal ontwikkelen.
Niettemin is het van groot belang dat de ontwikkeling van internationale regelgeving voor de elektronische snelweg voortgaat. Een meer generieke Lex Internet lijkt pas op termijn – als meer duidelijk is hoe de elektronische snelweg zich ontwikkelt – een interessante oplossing. Afhankelijk van de mogelijkheden van een internationaal verdrag zou Nederland wel eigen nationale normen kunnen ontwikkelen, die als voorbeeld zouden kunnen dienen voor latere internationale regelgeving. Belangrijke stappen in de richting van een Internetverdrag worden gezet door EU-commissaris Bangemann; hij onderzoekt de mogelijkheden van een breed uitgangspuntenstelsel voor de hele informatiesamenleving.

[1] Dit moet niet verward worden met de soms gehoorde wens de «nettiquette» te gebruiken als basis voor een Lex Internet. Nettiquette – de etiquette op het internet, met name geregeld in RFC 1855 – is daarvoor te beperkt. De nettiquette omvat voornamelijk regels voor gedrag op openbare gedeelten van het netwerk, met name over het plaatsen van usenet-postings en het reageren daarop. Voor complexe economische en technische regelgeving kan dat nauwelijks als basis dienen. Daarbij heeft de nettiquette onder meer als doel de commercie van het Internet te weren, wat een weinig bruikbaar uitgangspunt is voor bijvoorbeeld regulering van bedrijfsactiviteiten.

Het kabinet zal, gelet op het voorgaande, de internationale gedachtenvorming over een verdrag voor Internet bevorderen.

5.3. Zelfregulering

Een interessant alternatief voor (inter-)nationale regelgeving is het stimuleren van internationale zelfregulering door de belangrijkste actoren op het gebied van de elektronische snelweg. Immers, anders dan staten, zijn de belangrijkste actoren op Internet niet aan grenzen gebonden. Zelfregulering zou moeten worden gestimuleerd tezamen met die landen waarmee zich belangrijke betrekkingen ontwikkelen op de elektronische snelweg, waartoe in ieder geval de EU-lidstaten en de Verenigde Staten behoren. Dit alternatief verdient verder onderzoek. Daarbij moet ook worden gekeken naar de mogelijkheden voor een publiekrechtelijk toezicht op die zelfregulering, waarmee een sluitend en handhaafbaar regime mogelijk zou worden, dat bovendien kwetsbare belangen in voldoende mate beschermt.
De vraag naar internationale zelfregulering wordt klemmender naarmate de aangrijpingspunten voor nationale overheden verder afnemen. De verwachting dat in de nabije toekomst communicatie rechtstreeks van consument naar satelliet zal plaatsvinden, zonder tussenkomst van lokale service-providers, vereist internationale zelfregulering, zo nodig afgedwongen door overheden.

5.4. Oplossingen toepasbaar voor meerdere rechtsgebieden

Een belangrijke vraag ten slotte, is: in hoeverre moet worden gestreefd naar oplossingen die het gehele recht, of in ieder geval diverse rechtsgebieden omvatten? Voordelen van omvattende oplossingen zijn:
- Overeenkomstige typen problemen die zich in verschillende rechtsgebieden voordoen, kunnen op dezelfde manier worden opgelost.
- Overeenkomstige handelingen die in verschillende landen tot verschillende rechtsgebieden worden gerekend, kunnen op dezelfde manier worden opgelost.
- Het kan worden voorkomen dat waar dezelfde handeling effecten heeft op verschillende rechtsgebieden, de rechtsgevolgen uiteenlopen. Te denken valt aan een financiële transactie die fiscaal onder het recht van land A valt, privaatrechtelijk onder het recht van land B en strafrechtelijk onder het recht van land C.

Daar staat tegenover dat de eigenheden van verschillende rechtsgebieden ook in de elektronische omgeving moeten worden benut. Dit geldt zeker voor de mogelijkheid van rechtskeuze in het internationaal privaatrecht. Deze mogelijkheid doet zich qualitate qua niet voor in een aantal andere rechtsgebieden waar geen sprake is van twee partijen die vrijwillig tot overeenstemming komen.

6. Conclusies en voorstellen

Vanuit rechtsstatelijk oogpunt vormt de versnelde internationalisering van economie en samenleving één van de belangrijkere vraagstukken die door de komst van de elektronische snelweg worden opgeworpen. De meeste van de hier besproken kwesties rond rechtsmacht zijn alleen in internationaal verband op te lossen. Daarmee zijn zij in belangrijke mate onttrokken aan de greep van de nationale wetgever. Regeling van deze kwesties kan wel grote gevolgen hebben voor de werking en inhoud van de Nederlandse rechtsstaat. Zij vragen derhalve om een zorgvuldige inhoudelijke overweging en een gecoördineerde, tactische afstemming van de onderhandelingen, met name daar waar de gedane voorstellen rechtsgebiedoverstijgend zijn. In het actieplan in Deel V van de nota wordt aan dit uitgangspunt invulling gegeven.

6.1. Opeenstapeling van rechtsmachten

- Het kabinet streeft naar internationale harmonisatie van materiële normen. Daarbij zal het zijn inspanningen in eerste instantie richten op: economische ordeningswetgeving, het privaatrecht, vermogensdelicten, specifieke computerdelicten, vergrijpen waarover een brede internationale consensus bestaat, zoals kinderporno en extreem geweld en onderwerpen waarover een brede internationaal erkende gemeenschappelijke inzichten bestaan.
- Op langere termijn wordt ook voor wetgeving die is gebaseerd op culturele verschillen harmonisatie niet op voorhand afgewezen.
- Het ontstaan van vrijhavens valt niet geheel te voorkomen, maar de reikwijdte daarvan kan wel worden beperkt door een nadere regeling voor de aansprakelijkheid van tussenpersonen en door het opleggen van economische sancties. Het kabinet zal een en ander in internationaal verband nastreven.
- Het kabinet zal streven naar het opstellen van internationale regels over het uitoefenen van rechtsmacht. Indien dit niet haalbaar is, zal zij afspraken maken over onderlinge prioritering bij de uitoefening van rechtsmacht, waarbij naar analogie van de aanknopingsleer van het internationaal privaatrecht een oplossing zal worden gezocht.
- Het kabinet zal internationale organisaties, zoals UNCITRAL, UNIDROIT en de Internationale Kamer van Koophandel, aansporen om internationale privaatrechtelijke beginselen voor elektronische handel te definiëren. Hierbij zullen de deelnemers aan elektronische handel worden betrokken.
- Het kabinet zal hoge prioriteit geven aan het opstellen van Internet-iprregels in het kader van de Haagse Conferentie.

6.2. Handhaving van nationale wetgeving

6.2.1. Strafrecht

- Een goede samenwerking tussen opsporingsautoriteiten is vereist teneinde een effectieve handhaving te bereiken.
- Daartoe zal het kabinet afspraken maken teneinde op buitenlandse computers te kunnen opsporen en om de medewerking van andere landen bij de opsporing te verzekeren.
- Het wordt overwogen om af te zien van de eis van dubbele strafbaarheid bij het verlenen van rechtshulp, mits er geen sprake is van uitlevering. De rechtshulp zal uitsluitend zien op informatieverschaffing, teneinde het elektronisch spoor te kunnen traceren. Voorts dient te worden voldaan aan enkele andere voorwaarden: afspraken op basis van reprociteit, alleen rechtshulp bij van te voren bepaalde ernstige delicten, het delict zal moeten zijn gericht op de rechtsorde van het land dat om rechtshulp verzoekt en het achteraf inlichten van de betrokken persoon.

6.2.2. Privaatrecht

- Het leerstuk van de onrechtmatige daad biedt vooralsnog voldoende houvast om in Nederland gevestigde tussenpersonen aansprakelijk te stellen voor gepleegde onrechtmatige daden. Het kabinet zal de volgende specifieke onderwerpen onder de aandacht brengen van internationale organisaties, zoals de Raad van Europa.
- Het belang van het opstellen van een uniforme regeling voor de privaatrechtelijke aansprakelijkheid van tussenpersonen voor onrechtmatige daden.
- Het belang van reconstructie door de burger van een elektronisch

spoor, teneinde hem in staat te stellen te achterhalen waar vandaan jegens hem een onrechtmatige daad wordt gepleegd.

6.3. Overige onderwerpen

- In een beperkt aantal gevallen waarin het aanknopingspunt voor rechtsmacht een fysiek aangrijpingspunt is, schiet de rechtsmacht tekort. Dit fysieke aangrijpingspunt kan worden vervangen door een ander aangrijpingspunt, zoals:
  – de tussenpersoon, indien deze zich in Nederland bevindt en
  – de infrastructuur.
- Voor alle oplossingen geldt een voorkeur voor mondiale regeling. Vaak echter zal een mondiale regeling niet haalbaar zijn. Dan kunnen afspraken tussen de (westerse) geïndustrialiseerde landen een aanvaardbaar alternatief vormen.
- Een keuze voor nationale wetgeving kan evenwel onder de volgende omstandigheden zijn gerechtvaardigd:
  – ter bescherming van normen en waarden,
  – indien regelgeving op internationaal niveau niet haalbaar is, of te lang zou duren,
  – om de concurrentiepositie van Nederland te versterken, of
  – als voorbeeldfunctie voor de internationale rechtsontwikkeling.
- Een specifiek verdrag voor Internet is op dit moment niet aan de orde. Op dit moment moet internationale regelgeving zich richten op deelaspecten. Op langere termijn kan een Internetverdrag een goed alternatief zijn. Het kabinet zal de internationale gedachtenvorming daaromtrent bevorderen.
- Internationale zelfregulering door de belangrijkste actoren op het gebied van de elektronische snelweg vormt een interessant alternatief voor (inter-)nationale regelgeving. Zelfregulering verdient nader onderzoek, tezamen met de EU-lidstaten en de Verenigde Staten. Daarbij moet worden gekeken naar de mogelijkheden voor een publiekrechtelijk toezicht op die zelfregulering. Daarmee zou een sluitend en handhaafbaar regime mogelijk moeten worden, dat bovendien kwetsbare belangen beschermt.
- Voor problemen op verschillende rechtsgebieden moeten zoveel mogelijk gelijkluidende oplossingen worden gevonden. Het zal van de ontwikkeling van de elektronische snelweg afhangen of op langere termijn een meer fundamentele aanpak nodig is, waarbij aan soevereiniteiten moet worden getornd.

C. PRIVACY

1. Inleiding

In de informatiesamenleving zijn gegevens, dankzij digitale vastlegging, niet meer gebonden aan bepaalde fysieke dragers. Gegevens kunnen zeer snel worden getransporteerd en oneindig worden gekopieerd en gekoppeld. Hierbij treedt geen kwaliteitsverlies of beschadiging op. De aard van de gegevens speelt geen rol. Databanken met persoonlijke gegevens worden net zo makkelijk gekopieerd en gekoppeld als technische of juridische databanken.
Daarnaast laat iedereen die zich op de elektronische snelweg begeeft een elektronisch spoor achter. Dat spoor geeft inzicht in het doen en laten van personen, zonder overigens dat daarmee altijd direct de identiteit wordt onthuld. Moderne communicatie- en informatietechnieken dringen zodoende diep door in de persoonlijke levenssfeer, vaak zonder dat de gebruikers daar erg in hebben.
In de overgang naar de informatiesamenleving zijn vraagstukken van privacy daarom zeer belangrijk. Wat betekent het grondrecht op privacy nog in een samenleving waarin informatie en informatieproducten centraal staan? In hoeverre kan de overheid burgers een garantie bieden dat zij zeggenschap blijven houden over gegevens die hun persoonlijke leven betreffen?
Er bestaat geen consensus over de inhoud van het begrip privacy. Dat is ook bijna onmogelijk: privacy is in de eerste plaats een gevoel, dat deels afhankelijk is van tijdgeest en cultuur. De kern van het begrip ligt in de individuele behoefte aan bescherming van de persoonlijke levenssfeer. De vraagstukken omtrent privacy richten zich op de volgende onderdelen:

1. In de informatiesamenleving is de bescherming van persoonsgegeven een cruciale vorm van privacy, omdat het aantal registraties van gegevens sterk toeneemt en de verwerkingstechnieken steeds verfijnder worden.
2. In de informatiesamenleving wordt het lichaam steeds vaker als sleutel gebruikt voor de elektronische registratie en verificatie.
3. In de informatiesamenleving neemt het aantal elektronische contacten sterk toe. Aan de ene kant bestaat daarbij de behoefte om anoniem te blijven, terwijl anderzijds ook de bescherming van diezelfde persoonlijke levenssfeer kan meebrengen, dat men de mogelijkheid wil hebben om communicatiepartners te identificeren, bijvoorbeeld om elektronische stalking te voorkomen. In dit hoofdstuk is er daarom een aparte paragraaf opgenomen over de spanning tussen de behoefte aan anonimiteit en het belang van identificatie.
4. In de informatiesamenleving rijst de vraag in hoeverre het klassieke brief-, telefoon- en telegraafgeheim kan worden uitgebreid tot de nieuwe communicatiemiddelen.

Privacywetgeving vindt een basis in de Grondwet. Artikel 10 omschrijft het grondrecht privacy zelf. Verder zijn van belang artikel 11 betreffende de onaantastbaarheid van het menselijk lichaam, het huisrecht (artikel 12) en het brief-, telefoon- en telegraafgeheim (artikel 13). Deze bepalingen kunnen worden gezien als verbijzonderingen van het algemene recht op privacy.
Op Europees niveau ligt de basis in art. 8 EVRM[1] en de daarbij behorende jurisprudentie van het Europese Hof voor de rechten van de mens, alsmede het Verdrag van de Raad van Europa over persoonsgegevens[2]. Voor een uitgebreid overzicht van het juridisch instrumentarium dat betrekking heeft op privacy, wordt verwezen naar diverse onderdelen van Deel II C-4 van deze nota.

[1] In art. 8 EVRM is het recht op respect voor het privéleven van het individu neergelegd. Dit artikel heeft rechtstreekse werking.
[2] Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Raad van Europa.

2. Bescherming van persoonsgegevens

De kern van het probleem van de bescherming van persoonsgegevens wordt gevormd door de toename van het aantal registraties van persoonsgegevens, terwijl ook de gegevensverwerkende technologie steeds beter wordt. Hierdoor neemt het risico op inbreuken op de persoonlijke levenssfeer toe, terwijl het voor de burger steeds moeilijker te achterhalen wordt wie met welk doel persoonsgegevens verzamelt en verwerkt. Dit staat op gespannen voet met door de wetgever erkende principes als transparantie van gegevensverwerking en doelgebonden gegevensverwerking. Ook het toezicht door de burger en de Registratiekamer wordt steeds moeilijker. Steeds meer burgers maken gebruik van steeds meer organisaties en instellingen. Die instellingen leggen op hun beurt weer verfijndere registraties aan. Het resultaat is een explosie van persoonlijke dataregistraties.
Er zijn verschillende manieren waarop burgers in zon registratie terecht kunnen komen:

- *Bewuste registratie:* het actief achterlaten van gegevens.
- *Onbewuste registratie:* het onbedoeld achterlaten van gegevens.
- *Primaire vastlegging:* vastlegging bij de instantie die gegevens verzamelt.
- *Secundaire vastlegging:* overdracht van gegevens aan een derde instantie.

Deze manieren van registratie kunnen gecombineerd voorkomen. Voorbeelden:

	Primair	Secundair
Bewust	Inschrijving als lid van een vereniging	Vereniging draagt ledenbestand over aan andere instantie, met toestemming van de leden
Onbewust	Bezoeken van een website die e-mail adres en server van oorsprong vastlegt	Beheerder website draagt (schaduw-) bezoekersregister over aan andere instantie zonder toestemming geregistreerden

Voorts vergemakkelijken de mogelijkheden om bestanden te koppelen en de geavanceerde technieken voor inrichting en ontsluiting van gegevensbestanden het terugzoeken van gegevens op meerdere criteria. Hierdoor kan tegelijkertijd nieuwe informatie over geregistreerden worden gegenereerd. Overheden, bedrijven en medeburgers beschikken daarmee over een krachtig hulpmiddel om zich inzicht te verschaffen in de persoonlijke levenssfeer van anderen. Ook zijn er technische middelen, zoals beeld- en geluidsopnameapparatuur, die zeer eenvoudig inbreuk kunnen maken op de persoonlijke levenssfeer. Met behulp van informatietechnologie is het – indien aan bescherming van bestanden en persoonsgegevens niet veel aandacht wordt besteed – dus niet moeilijk om een zeer gedetailleerd beeld te krijgen van de activiteiten, financiële handel en wandel, voorkeuren en gewoonten van de gemiddelde of individuele burger, zonder dat deze daarmee heeft ingestemd.
Daartegenover staat dat diezelfde technologie de burger ook de mogelijkheid biedt zich onzichtbaar te maken voor de overheid en andere partijen. Tegenover de technisch geavanceerde zoek- en koppelingsmethoden staan namelijk technieken die gegevens versluieren en ontoegankelijk maken – encryptie, steganografie – en technieken en produkten die het anoniem optreden van de burger in een elektronische omgeving verzekeren, zoals de anonymous re-mailers, anonymous servers en call-cards voor mobiele telefoons. Daarnaast bieden geavanceerde en goedkope communicatiemiddelen iedereen de mogelijkheid om activiteiten in de elektronische omgeving te verplaatsen naar het buitenland. Hierdoor kunnen zij zich onttrekken aan de rechtsmacht van

het land waarin zij zijn gevestigd. Een toekomst waarin burgers zich kunnen en ook mogen hullen in een elektronische mantel werpt echter voor de overheid ook andere vragen op. Deel III F van deze nota behandelt een aantal van deze vragen, met het oog op de handhaving.
Voor de overheid zijn op het terrein van de bescherming van persoonsgegevens drie taken weggelegd:

- Vergroting van het privacybewustzijn en de zelfbescherming van de burger.
- Het stimuleren en ondersteunen van zelfregulering op elektronische markten.
- Het bevorderen van internationale harmonisatie van normen en instrumenten.

2.1. Vergroting van het privacybewustzijn en de zelfbescherming van de burger

Hoewel de effectiviteit van de Wet bescherming persoonsgegevens (Wbp) pas duidelijk zal worden nadat geruime tijd met deze wet ervaring is opgedaan, is de verwachting dat toekenning van handhavingsinstrumenten aan de Registratiekamer niet de enige oplossing is voor handhaving van de Wbp.
Veel inspanningen zullen moeten worden gericht op het transparant maken van de gegevensverwerking voor de burger, opdat de burger in staat zal zijn controle uit te oefenen op verwerking van de hem betreffende gegevens. Onderzoek heeft aangetoond dat geregistreerden veel waarde hechten aan de aan hen toegekende rechten, zoals inzage, correctie en verwijdering. Dit om zicht te houden op de verwerking van de hen betreffende persoonsgegevens. In concrete situaties is echter gebleken dat zij niet of nauwelijks hun rechten weten te effectueren, bijvoorbeeld op Internet. Internet kent immers geen duidelijke structuur en nauwelijks controle. Van een doorzichtige verantwoordelijkheidsstructuur is al helemaal geen sprake, doordat veel verschillende bedrijven toegang tot het Internet verlenen. Verbetering van de transparantie voor de burger wordt bij inwerkingtreding van de Wbp verwacht door een aangescherpte informatieplicht en het inzetten van de handhavingsinstrumenten door de Registratiekamer.
De overheid kan het echter niet laten bij het stellen van regels die transparantie van gegevensverwerking moeten bewerkstelligen. Allereerst moeten burgers meer betrokken worden bij de verwerking van hen betreffende persoonsgegevens. Zij dienen zich enerzijds bewust te zijn van gegevensverwerking; anderzijds moeten zij zelf in staat te zijn controle uit te oefenen op de verwerking daarvan. De overheid moet hieraan, in samenspraak branche-organisaties van gegevensverwerkende bedrijven, een bijdrage leveren door middel van voorlichting over:

- de rechten die burgers hebben als hun persoonsgegevens worden verwerkt;
- de verplichtingen die verantwoordelijken ten aanzien van geregistreerden hebben;
- de mogelijkheden die burgers hebben om hun privacy in een elektronische omgeving af te schermen, bijvoorbeeld door het gebruik van beveiligingstechnieken.

De betrokkenheid van de burger kan vervolgens worden ondersteund door de burger (meer dan thans het geval is) zelf het specifieke niveau van bescherming van persoonsgegevens te laten bepalen. Zo wordt de abonnee in het voorstel voor een nieuwe Telecommunicatiewet de mogelijkheid geboden om zelf keuzes te maken over de mate waarin persoonsgegevens worden gebruikt. Ingevolge dit wetsvoorstel kan de burger onder meer beslissen om gespecificeerde nota's te ontvangen, of ongeïdentificeerde oproepen te weigeren. Ook kan hij zelf bepalen of hem

betreffende gegevens, zoals met wie, wanneer en waarvandaan hij belt, voor uiteenlopende doelen kunnen worden gebruikt. In toekomstige wetgeving moet dan ook, zodra vanuit privacyoverwegingen een sector-specifieke regeling noodzakelijk wordt geacht, meer dan nu het geval is, worden bekeken of het mogelijk is de burger zelf het niveau van bescherming te laten bepalen. Het vertrouwen in een juiste bescherming van persoonsgegevens zal daarmee kunnen toenemen, hetgeen van groot belang is voor de verdere groei en ontwikkeling van de elektronische snelweg.
De uitoefening van aan burgers toegekende rechten dient voorts door de overheid te worden gefaciliteerd. Dit omdat het voor de burger in de informatiematiemaatschappij steeds moeilijker te achterhalen wordt wie welke gegevens met welk doel verwerkt. Veelal zal de burger pas worden geconfronteerd met gegevensverwerking als hij, zonder daarom te hebben verzocht, direct wordt aangeschreven. Het probleem zal zich met name voordoen bij direct marketing. Voor het uitoefenen van het «opt-out-recht»[1] kan de burger zich thans wenden tot de Nederlandse associatie voor direct marketing, distance selling en sales promotion (DMSA), die de burger de mogelijkheid biedt op te geven niet meer telefonisch te willen worden benaderd. De DMSA dekt evenwel niet de gehele markt en voorziet alleen in het uitoefenen van het «opt-out»-recht voor telefonische commerciële aanbiedingen. Om de burger te helpen bij het uitoefenen van zijn recht, zal het kabinet de oprichting van een aanspreekpunt voor burgers die niet willen worden gestoord in verband met commerciële aanbieding bevorderen. Oprichting dient plaats te vinden langs de weg van zelfregulering door diverse branches.

2.2. Het stimuleren en ondersteunen van zelfregulering op elektronische markten

Aansluitend op het naleven en handhaven van de Wbp door de Registratiekamer en de burgers zelf, is zelfregulering door marktpartijen essentieel. Door betrokkenen kan nadere invulling worden gegeven aan de normen uit de Wbp. Voor burgers wordt dan duidelijk of er persoonsgegevens worden verwerkt, door wie en aan welke voorwaarden dat is gebonden. Daardoor zullen burgers en medewerkers beter in staat zijn om hun rechten te effectueren. Het opzetten van het bovengenoemde aanspreekpunt is een onderdeel van deze zelfregulering.
Ook vanuit de Raad van Europa worden initiatieven genomen om zelfregulering te stimuleren. Zo is in maart 1997 door het «Bureau of the project on data protection» de «draft code of practice for Internet service providers» opgesteld. Deze ontwerp-code bevat de belangrijkste uitgangspunten die ten grondslag liggen aan de privacybescherming in Europa zoals die zijn verwoord in de EG privacyrichtlijn. Het kabinet zal deze vorm van zelfregulering verder stimuleren, waarbij een gedragscode voor Internetproviders voorrang heeft. Zij beschikken immers over een schat aan persoonsgegevens, waarbij het voor de buitenwereld ondoorzichtig is welke gegevens worden verzameld en waarvoor deze worden gebruikt. Het moet worden overwogen of van hen tevens mag worden verwacht dat ze de identiteit van een informatieleverancier kunnen nagaan. Het belang hiervan is dat de ondoorzichtigheid, die wordt veroorzaakt doordat op Internet vele mogelijkheden bestaan om de identiteit te camoufleren enigszins kan worden doorbroken. De burger krijgt zo een aangrijpingspunt om te achterhalen wie er zit achter een anoniem aanbod, of achter de verwerking van hem betreffende persoonsgegevens.
De Wbp introduceert naast de gedragscode nog een ander instrument dat de transparantie van gegevensverwerking ten goede kan komen. Het betreft hier de «functionaris voor de gegevensbescherming». Iedere verantwoordelijke – of organisatie van verantwoordelijken – kan een eigen privacyfunctionaris benoemen. Deze privacyfunctionaris heeft tot taak toe

[1] Het opt-out recht betekent dat als degene wiens gegevens worden verwerkt bezwaar maakt tegen deze verwerking, dit bezwaar moet worden gehonoreerd, ongeacht of er sprake is van een gerechtvaardigd individueel belang. In geval van gegevensverwerking in de direct marketing branche kunnen burgers dit recht uitoefenen.

te zien op de verwerking van de persoonsgegevens en eventueel op de naleving van de gedragscode. Die functionaris kan tevens als aanspreekpunt fungeren voor burgers die iets willen weten over hun persoonsgegevens, of die hun rechten willen uitoefenen. Immers, het zal van een burger veelal heel wat inspanning vergen om te achterhalen tot wie hij zich binnen een organisatie moet wenden voor bijvoorbeeld een verzoek om inzage. Het kabinet zal zich daarom in nauw overleg met de Registratiekamer ervoor inzetten dat zoveel mogelijk privacy-functionarissen worden benoemd, die naast de aan hen in de Wbp toegekende taak tevens fungeren als aanspreekpunt voor burgers.

2.3. Het bevorderen van harmonisatie van normen en instrumenten

Privacynormen en instrumenten zijn binnen Europa in zekere mate geharmoniseerd. De lid-staten hebben echter nog steeds veel ruimte de open privacynormen zelf in te kleuren. Daarom is het noodzakelijk de implementatie-initiatieven van de lidstaten op de voet te volgen. Zodra blijkt dat invulling van normen op belangrijke terreinen – bijvoorbeeld bij het verzekerings- en bankwezen – te ver uit elkaar lopen, zal het kabinet sectorale invulling van de algemene normen nastreven. Pas dan zal er een dekkend regime voor de bescherming van persoonsgegevens binnen Europa kunnen ontstaan.
Het realiseren van geharmoniseerde privacynormen binnen Europa is een belangrijke stap naar verdergaande internationale harmonisering. Juist op dat niveau is het vertrouwen van de consument in een juiste omgang met en bescherming van persoonsgegevens noodzakelijk voor de verdere ontwikkeling van de elektronische snelweg. De elektronische snelweg is immers een internationaal fenomeen en de economische voordelen die de elektronische snelweg kan bieden, kunnen pas volledig worden benut als ook internationaal de bescherming van persoonsgegevens is geharmoniseerd. Harmonisatie zal in eerste instantie in OESO-verband moeten worden gerealiseerd. Dan kan worden aangesloten bij de Guidelines on the protection of privacy and transborder flows of personal data. Deze Guidelines zullen wel nog nader moeten worden ingevuld. Vanuit Europa zou de ervaring die is opgedaan in het kader van de harmonisatie van privacynormen als «best practice» kunnen dienen. Het kabinet realiseert zich echter ook dat op dit punt tussen de VS en de EU belangrijke verschillen van mening bestaan. Indien wereldwijde harmonisatie niet mogelijk is, dient verdere harmonisatie in EU-verband te worden nagestreefd.

3. Biometrische persoonsgegevens en het recht op onaantastbaarheid van het menselijk lichaam

Biometrie is een vorm van persoonsherkenning of -verificatie aan de hand van een uniek lichamelijk kenmerk. Op de elektronische snelweg wordt op dit moment voor persoonsherkenning of persoonsverificatie vooral gebruik gemaakt van de PIN-code. De PIN-code levert eigenlijk geen persoonsverificatie op, omdat de code kan worden overgedragen of gestolen. De verwerkende machine controleert echter niet wie de PIN-code gebruikt.
Burger en overheid hebben behoefte aan een echte persoonsherkenning op de elektronische snelweg. Immers, handhaving van bestuursrecht en strafrecht door de overheid en handhaving van het burgerlijk recht door civiele partijen is afhankelijk van de mogelijkheid vast te stellen wie een persoon precies is.
Hier staat de vraag centraal of biometrie niet op gespannen voet staat met art. 11 van de Grondwet, waarin het absolute recht op onaantastbaarheid van het menselijk lichaam is vastgelegd. Dit artikel geeft ruimte voor beperkingen van dit recht bij, of krachtens de wet. Biometrische persoons-

verificatie bij of krachtens wettelijk voorschrift hoeft dus niet op gespannen voet te staan met het recht op onaantastbaarheid van het lichaam.
In het algemeen[1] eist de wet voor biometrische persoonsverificatie toestemming van betrokkene. Na inwerkingtreding van de Wet bescherming persoonsgegevens is toestemming niet voldoende voor een biometrische persoonsverificatie met een lichaamskenmerk waaruit raskenmerken of etnische herkomst kunnen worden afgeleid. Bij een aantal biometrische technieken is dit het geval, zoals bij gezichtsherkenning met foto of video. Voor deze zogenoemde gevoelige persoonsgegevens geldt in de toekomst een verbodsstelsel. Het verbod is alleen niet van toepassing indien deze vorm van persoonsverificatie onvermijdelijk is.
In het algemeen lijkt een dergelijk stelsel geschikt om te voorkomen dat biometrische persoonsverificatie in conflict zal komen met de wettelijke bescherming van de privacy. Er moet worden onderzocht of een bagatelregeling nodig is voor kleinschalig gebruik van biometrische persoonsgegevens die qua aard moeten worden gezien als «gevoelig» in de zin van de Wbp, maar in de praktijk reeds zijn ingeburgerd.
De portee van de biometrie voor de elektronische snelweg reikt aanzienlijk verder dan alleen de aantasting van het menselijk lichaam. Biometrische persoonsverificatie kan op de elektronische snelweg de burger een betere beveiliging bieden van gegevens die belangrijk zijn voor zijn persoonlijke levenssfeer. Niet alle biometrische persoonsverificatieprocedures zijn gepersonaliseerd. Zogeheten anonieme biometrie geeft een sluitende persoonsverificatie zonder direct te openbaren wie de betrokkene is. Het gebruik van anonieme biometrie is dan ook in het belang van de privacy.

Voor gepersonaliseerde biometrie is in een aantal gevallen overheidsbemoeienis gerechtvaardigd. Vooral gepersonaliseerde biometrie op een multifunctionele chipcard zal – mede ter bescherming van de privacy – moeten berusten op deugdelijk onderzoek naar de ware identiteit van de persoon. Hiervoor is een wettelijke verankering vereist, in eerste instantie in de Wet op de identificatieplicht. Daarnaast komen ook sectorspecifieke wetten die zich op de sectorale identificatieplicht richten in aanmerking. Deze wetten worden hieronder in 4.1 beschreven.
Door gepersonaliseerde biometrie via de Wet op de identificatieplicht te koppelen aan identificatieplicht voor de personaliserende instantie en aan legitimatieplicht voor de betrokkene, zal gepersonaliseerde biometrie slechts voor een beperkt aantal toepassingen worden gebruikt. Daarnaast heeft een duidelijk onderscheid tussen anonieme en gepersonaliseerde biometrie op zichzelf al een ordenende werking. Toepassing van gepersonaliseerde biometrie zal worden beperkt ten gunste van anonieme biometrie, die steeds vrij kan worden toegepast.
Het kabinet stelt voor het personaliseren van chipkaarten en andere elektronische identiteitsbewijzen onder de werking van de Wet op de identificatieplicht en achterliggende specifieke wetten te brengen.
Voor kleinschalige elektronische toepassingen kan met een bagatelregeling worden volstaan.

Persoonsverificatie met grootschalige biometrische technieken is voor de overheid een nieuw fenomeen. Een ITER-onderzoek concludeert dat een nadere regeling van biometrische technieken en databanken met biometrische persoonskenmerken niet in alle opzichten aan particuliere partijen op de vrije markt kan worden overgelaten. Voor zover het daarbij gaat om standaardisatie, kan met vormen van zelfregulering worden volstaan, bij voorkeur in internationaal verband. Het kabinet is echter van mening dat met het oog op bescherming van de persoonlijke levenssfeer en de privacy van personen een nadere wettelijke regeling voor de opslag

[1] Deze samenvatting is gebaseerd op Van Kralingen, Prins en Grijpink, 1997.

en het gebruik van biometrische gegevens noodzakelijk is. Internationale regelgeving is daartoe gewenst.

4. Anonimiteit en identiteit

4.1. Anonimiteit versus identiteit

In het gewone maatschappelijke verkeer kunnen burgers zich in beginsel anoniem op de openbare weg bewegen. Het vragen naar de identiteit is voorbehouden aan personen die daartoe op grond van de wet zijn bevoegd. Bij de Wet op de identificatieplicht is een aantal wetten uitdrukkelijk voorzien van een identificatieplicht voor de uitvoerende instantie en een legitimatieplicht voor de betrokkene[1]. Daarnaast bevat het Wetboek van Strafrecht een algemene regeling.
De realiteit op de elektronische snelweg is dat deelnemers daaraan altijd persoonsgegevens achterlaten die op enigerlei wijze inzicht geven in hun persoon. Zonder dat daarmee overigens direct de identiteit wordt onthuld. Het gaat dan meestal om technische gegevens en administratieve kenmerken, bijvoorbeeld de zogeheten «calling line identification»[2]. In een aantal gevallen zal de wet of het maatschappelijk functioneren verplichten tot het vaststellen van iemands identiteit.
De elektronische snelweg vergroot zowel de behoefte aan een meer persoonsgebonden identiteitsvaststelling, als aan anoniem deelnemen aan het elektronisch verkeer. Daarbij blijft het huidige uitgangspunt in het maatschappelijke verkeer in feite ongewijzigd: voor zover de wet – bijvoorbeeld bij het afsluiten van wettelijk verplichte verzekeringen – of het maatschappelijk functioneren – bijvoorbeeld het afsluiten van bepaalde overeenkomsten – niet noodzaakt tot opheffing van de identiteit, moet anonimiteit op de elektronische snelweg het uitgangspunt zijn.

4.2. Biometrie voor anonimiteit en identiteit

Het gebruik van biometrische persoonsverificatie kan in beide behoeften voorzien. Het verschil zit niet in het biometrische kenmerk zelf, maar in de gerelateerde identificerende persoonsgegevens. Een losse biometrische «template»[3] is niet aan te merken als een persoonsgegeven; de wetgeving aangaande persoonsgegevens is derhalve niet van toepassing en deze niet-gepersonaliseerde, anonieme vorm van biometrische persoonsverificatie is dus vrij toepasbaar[4]. Opslag van zon biometrisch template op een chipcard en gebruik daarvan voor «off-line»-verificatie, is onbeperkt mogelijk. Dit ligt anders wanneer het template wordt gekoppeld aan andere gegevens die wel als persoonsgegevens kunnen worden aangemerkt, of die tot persoonsgegevens kunnen worden herleid.
Anonieme biometrie – handpalmgetal met PIN-code, bijvoorbeeld – biedt aan de ene kant de mogelijkheid voor persoonsverificatie, terwijl aan de andere kant het ontbreken van identificerende persoonsgegevens het onmogelijk maken ter plaatse vast te stellen om wie het precies gaat. Voor veel maatschappelijke doeleinden kan met dit type persoonsverificatie worden volstaan. Indien het maatschappelijk doel geen anoniem verkeer verdraagt, ligt gebruik van gepersonaliseerde biometrie voor de hand.

De gevolgen van de toepassing van biometrie kunnen voor de burger ingrijpend zijn. Uit oogpunt van rechtszekerheid zal het kabinet een voorstel doen voor een algemene wettelijke basis voor het gebruik van biometrie voor de uitvoering van publieke taken. Dit voorstel sluit aan bij het voorstel voor aanpassing van de Wet op de identificatieplicht (zie hierboven onder 3).

Naarmate de communicatie tussen de overheid en burger en tussen burgers onderling meer via de elektronische snelweg plaatsvindt, is het

[1] In de verhouding overheid–burger wordt thans in diverse wetten de identificatieplicht geregeld. Het Wetboek van Strafrecht, de Organisatiewet sociale verzekering, de Algemene bijstandswet, de Algemene wet inzake rijksbelastingen en de Wet personenvervoer zijn van die wetten. De Wet op de identificatieplicht wijst vervolgens de documenten aan die gebruikt kunnen worden ter vaststelling van de identiteit, zoals het paspoort en rijbewijs. Ook in de relatie van burgers onderling schrijft een viertal wetten een identificatieplicht voor. Dit betreft de Wet arbeid buitenlandse werknemers, de Wet inzake spaarbewijzen, de Wet identiteitsvaststelling bij financiële dienstverlening en de Wet op het notarisambt.

[2] In de ontwerp-richtlijn van de EG (Gemeenschappelijk standpunt (EG) nr. 57/96) worden telecommunicatie-organisaties verplicht abonnees een technische voorziening aan te bieden waardoor deze op eenvoudige wijze per oproep de identificatie van het nummer dat zij gebruiken, onmogelijk kunnen maken. Deze voorziening zou slechts kunnen worden doorbroken in geval van een bevoegd gegeven bevel tot onderscheppen en verstrekken van de desbetreffende gegevens met het oog op opsporing van strafbare feiten of in het belang van de staatsveiligheid.

[3] Een biometrisch template is getal dat met een bepaald algoritme berekend is uit een biometrische afbeelding (vingerafdruk, handpalmvorm of handtekeningsbeweging); vanuit dit getal kan de oorspronkelijke afbeelding niet meer worden gereconstrueerd. Tegenover een tempplate staat het volledige analoge biometrische signaal in de vorm van een afbeelding (vingerafdruk of handpalmvorm), meting (handtekeningbeweging) of geluidsopname (stem).

[4] Deze conclusie is gebaseerd op: Van Kralingen, Prins en Grijpink, 1997.

eigenaardig dat wanneer burgers wettelijk verplicht zijn zich te identificeren, dit alleen kan – zoals de Wet de op identificatieplicht dat voorschrijft – door middel van een schriftelijk document. Voor het schriftelijk identificerende document moet daarom een elektronisch equivalent worden gezocht, dat dezelfde waarborgen biedt als het gaat om het vaststellen van de identiteit. Het gebruik van een gedigitaliseerd biometrisch gegeven, in combinatie met identificerende persoonsgegevens – naam, geboortedatum, geboorteplaats, etc. – kan hierin tegemoet komen.

4.3. Ondersteuning privacy door de techniek

Bepaalde technieken maken het mogelijk om registraties, waarvoor het niet is vereist dat de identiteit van de registreerde bekend is, zoveel mogelijk te anonimiseren. Deze technieken worden ook wel aangeduid als «privacy enhancing technologies», PET. Met name vanuit de Registratiekamer wordt voor PET veel aandacht gevraagd. Op zich doen PET niet meer dan uitvoering geven aan de algemene uitgangspunten van privacy-bescherming. Desalniettemin vormen zij een belangrijke impuls om zo min mogelijk persoonsidentificerende gegevens te verwerken. De belangrijkste conclusie van het rapport van de Registratiekamer «privacy enhancing technologies»[1], luidt dat met behulp van de huidige informatie- en communicatietechnologie systemen kunnen worden ontwikkeld voor dienstverlening, informatievoorziening en betaling. Daarbij worden veel minder persoonsgegevens verwerkt dan nu meestal het geval is. Deze conclusie onderstreept het belang van PET voor de bescherming van de persoonlijke levenssfeer in een informatiesamenleving. Nu deze technieken ter beschikking staan, moet kritischer worden gekeken naar de inrichting van databases en naar het doel van de verwerking van identificerende persoonsgegevens. Als het doel dit niet rechtvaardigt, moet meer gebruik worden gemaakt van PET. Van overheidszijde moet het gebruik van deze technieken worden gestimuleerd. De overheid moet daarbij als verantwoordelijke van velerlei registraties het goede voorbeeld geven.
De introductie van deze technieken mag er echter niet toe leiden dat afbreuk wordt gedaan aan de taak en mogelijkheden van opsporende en toezicht houdende overheidsinstanties, of aan het belang van de veiligheid van de staat. Daarom is het van groot belang dat er bij toepassing van PET altijd een mogelijkheid aanwezig is om de gegevens naar personen terug te herleiden.

5. Vertrouwelijkheid van communicatie

Voor zover de bescherming van de persoonlijke levenssfeer bestaat uit het beschermen van communicatie die als vertrouwelijk moet worden aangemerkt, onderscheidt de Grondwet in artikel 13 thans een drietal communicatiemiddelen: de brief, de telefoon en de telegraaf. Doordat deze bepaling technologie-afhankelijk is geformuleerd, is artikel 13 met de komst van de elektronische snelweg gedateerd geraakt.

5.1. De vertrouwelijkheid van e-mail

Vooral de vraag of e-mail onder de bescherming van artikel 13 valt, heeft veel aandacht gekregen. Voor een goed begrip van deze discussie is het noodzakelijk allereerst vast te stellen wat of wie de beschermwaardigheid van communicatie bepaalt.
Bij de beantwoording van deze vraag zou eerst kunnen worden gekeken naar de inhoud van een bericht. Dit biedt echter geen oplossing, omdat informatie die als zeer vertrouwelijk kan worden aangemerkt, toch regelmatig wordt verspreid. Men denke hierbij aan wat gasten van

[1] Opgesteld in samenwerking met TNO-FEL (Fysisch en Elektronisch laboratorium) en de Information and Privacy Commissioner van Ontario te Canada.

tv-talkshows vertellen. De wil van degene die het bericht verspreidt, biedt daarom een beter aanknopingspunt. Het is echter ondoenlijk om bij elk uitgewisseld bericht vast te stellen wat de wil van de betrokken personen is. Wel is het mogelijk om de achterliggende wil op basis van de context waarin een bericht wordt uitgewisseld te achterhalen. Deze benadering is gekozen bij de regeling van de bescherming van het brief-, telefoon- en telegraafgeheim. Zodra iemand bijvoorbeeld een bericht in een gesloten envelop stopt, kan er vanuit worden gegaan dat de achterliggende wil gericht is op overbrenging zonder inmenging van derden.
Kortom, niet de inhoud van het bericht bepaalt de bescherming, maar het omhulsel. Dit uitgangspunt wordt ook gehanteerd bij strafrechtelijke bepalingen die tot doel hebben communicatie en informatie tussen burgers onderling te beschermen. Als voorbeeld hiervan kan de bescherming van het briefgeheim (artikel 201 van het Wetboek van Strafrecht) worden genoemd en de bescherming van geautomatiseerde werken, de zogenoemde computervredebreuk (artikel 138a van het Wetboek van Strafrecht).
Het kabinet heeft naar aanleiding van het verslag bij het wetsvoorstel tot wijziging van artikel 13 Grondwet[1] in de nota een verduidelijking gegeven over de status van e-mail. De geobjectiveerde wil tot geheimhouding blijft hierbij het uitgangspunt. Of daarvan sprake is, wordt bepaald door het criterium of een derde een «hindernis» moet nemen, teneinde kennis te nemen van de inhoud van de communicatie. Van een dergelijke hindernis is sprake indien die derde het bericht moet ontsleutelen of een code moet breken. In de praktijk blijkt dat alle e-mail in ieder geval met een password is beveiligd: zowel bij de verzender, de provider, als bij ontvanger. E-mail wordt derhalve altijd als beschermwaardig aangemerkt en valt dan ook onder de bescherming van het voorgestelde artikel 13. Aangenomen moet worden dat deze benadering blijft gelden in de tekst van het artikel zoals dit geamendeerd door de Tweede Kamer is ontvangen.

5.2. De strafrechtelijke bescherming van e-mail

Voor de strafrechtelijke bescherming van e-mail moet een onderscheid worden gemaakt tussen de fase van het transport van e-mail over een telelcommunicatienetwerk en de fase van opslag van een e-mail op een computer. In de eerste fase is e-mail, net als elk ander telecommunicatie-verkeer, beschermd. Daarvoor geldt een aftapverbod (artikelen 139c en 374 bis van het Wetboek van Strafrecht). Opgeslagen e-mail geniet eveneens bescherming, nu in de praktijk alle opgeslagen e-mail met een password is beveiligd. Het doorbreken van deze beveiliging is strafbaar gesteld in artikel 138a (computervredebreuk). Onduidelijk is echter of een Internetprovider zich schuldig zou maken aan computervredebreuk als hij zonder toestemming in de mailboxen van zijn abonnees zou kijken. De Internetprovider is immers eigenaar van het geautomatiseerde werk waarop de mailbox zich bevindt. Daarom is het de vraag of er sprake zou zijn wederrechtelijk binnendringen in het geautomatiseerde werk door de provider. In het voorontwerp van de Wet computercriminaliteit II wordt dan ook voorgesteld om Internetproviders te verbieden kennis te nemen van bij hen opgeslagen e-mailberichten. Daartoe wordt artikel 372 van het Wetboek van Strafrecht aangepast.
Ook in de bescherming van e-mail in de verhouding van burger en overheid wordt voorzien. In een regeling voor het onderscheppen van e-mail in de fase van transport was al voorzien door het aftapverbod. In het voorontwerp van de Wet computercriminaliteit II wordt nu voor wat betreft opgeslagen e-mail voorgesteld de eisen die gelden voor justitieel onderzoek van poststukken door te trekken naar het justitieel onderzoek van e-mail, waartoe artikel 125i van het Wetboek van Strafvordering dient te worden gewijzigd. Artikel 125i van het Wetboek van Strafvordering (onderzoek van gegevens in een geautomatiseerd werk) is namelijk,

[1] IIK 25 433.

vergeleken bij de regeling van de inbeslagneming van (stoffelijke) geschriften, te algemeen gesteld voor wat betreft het onderzoek van e-mail. De voorgestelde wijziging van artikel 125i betekent onder meer dat alleen justitieel onderzoek van e-mail kan plaatsvinden met toestemming van de rechter-commissaris.

6. Conclusies en voorstellen

De invloed van ICT op privacy ligt vooral in de bescherming van persoonsgegevens, biometrische kenmerken, de persoonlijke communicatie en op de mate waarin burgers zich anoniem op de elektronische snelweg kunnen begeven. Hieronder zullen de belangrijkste conclusies en voornemens worden aangegeven.

6.1. De bescherming van persoonsgegevens

- In toekomstige wetgeving moet, zodra vanuit privacyoverwegingen een sector-specifieke regeling noodzakelijk wordt geacht, meer dan thans het geval is, worden bezien of het mogelijk is de burger zelf het niveau van privacybescherming te laten bepalen.
- Voorlichting over de aan de geregistreerde toegekende rechten en over verplichtingen van verantwoordelijkheden ten aanzien van geregistreerden en over de mogelijkheden om zelf met behulp van beveiligingstechnieken persoonsgegevens af te schermen.
- Het kabinet zal de oprichting van een aanspreekpunt voor burgers die niet willen worden gestoord in verband met commerciële aanbiedingen bevorderen. Oprichting moet plaatsvinden langs de weg van van zelfregulering door diverse branches. Het initiatief van de direct-marketing-branche kan hierbij als voorbeeld dienen.
- Het kabinet zal op dit terrein zelfregulering in internationaal verband verder stimuleren. Daarbij heeft een internationale gedragscode voor Internetproviders voorrang.
- Het kabinet zal zich, in nauw overleg met de Registratiekamer, ervoor inzetten zoveel mogelijk privacyfunctionarissen te benoemen, die naast de wettelijke opgedragen taak tevens zullen fungeren als aanspreekpunt voor burgers.
- Indien blijkt dat de invulling van de normen op belangrijke terreinen, zoals bijvoorbeeld bij het verzekerings- en bankwezen, binnen de lidstaten van de EU te ver uit elkaar loopt, zal het kabinet sectorale invulling van de algemene normen voor gegevensbescherming nastreven.
- Het kabinet streeft naar verregaande internationale harmonisatie van normen. In eerste instantie zal daarbij worden aangesloten bij de in OESO-verband ontwikkelde «Guidelines on the protection of privacy and transborder flows of personal data». Deze Guidelines zullen nader moeten worden ingevuld. Vanuit Europa zou de ervaring die is opgedaan in het kader van de harmonisatie van privacynormen als «best practice» kunnen dienen.

6.2. Biometrie en de onaantasbaarheid van het lichaam

- Biometrische verificatie bij of krachtens wettelijk voorschrift is niet strijdig met artikel 11 van de Grondwet. Voor gevoelige persoonsgegevens geldt in de toekomst een verbodsstelsel, op basis van de Wet bescherming persoonsgegevens.
- Er moet worden onderzocht of een bagatel-regeling nodig is voor kleinschalig gebruik van biometrische persoonsgegevens die qua aard moeten worden gezien als «gevoelig» in de zin van de Wbp, maar in de praktijk reeds zijn ingeburgerd.
- Het kabinet stelt voor het personaliseren van chipkaarten en andere

elektronische identiteitsbewijzen onder de werking van de Wet op de identificatieplicht en achterliggende specifieke wetten te brengen. Voor kleinschalige elektronische toepassingen kan met een bagatel-regeling worden volstaan.
- Het kabinet zal de totstandkoming van internationale afspraken over het gebruik van biometrische technieken en databanken met biometrische persoonskenmerken bevorderen. Voor zover het daarbij gaat om standaardisatie kan met vormen van zelfregulering worden volstaan.
- Het kabinet zal stappen ondernemen om in EU-verband te komen tot een nadere wettelijke regeling voor de opslag en het gebruik van gepersonaliseerde biometrische gegevens.

6.3. Anonimiteit en identiteit

- Het kabinet zal het gebruik van PET en anonieme biometrie stimuleren – in het bijzonder binnen de overheid. Hierbij geldt als restrictie dat indien hogere belangen (o.a. staatsveiligheid en voorkoming, opsporing en vervolging van strafbare feiten) dat vergen, de gegevens (terug) te herleiden moeten zijn naar concrete personen.
- Het kabinet zal stappen ondernemen voor de ontwikkeling van elektronisch equivalenten voor de schriftelijke en bij wet erkende, identificatiedocumenten (zie hiervoor ook Deel III D).
- Het kabinet zal een voorstel doen voor een algemene wettelijke basis voor het gebruik van biometrie voor de uitvoering van publieke taken.

6.4. Vertrouwelijkheid van communicatie

E-mail gaat volledige strafrechtelijke bescherming genieten. Naast het al bestaande aftapverbod van telecommunicatie, dat ook geldt voor e-mail in de transportfase, wordt in het voorontwerp van de Wet computercriminaliteit II voorgesteld het kennisnemen door een internet service provider van bij hem opgeslagen e-mail strafbaar te stellen. Ook wordt voorgesteld artikel 125i van het Wetboek van Strafvordering zo aan te passen dat voor het justitieel onderzoek van e-mail dezelfde eisen gelden als voor justitieel onderzoek van poststukken.

D. BETROUWBAARHEID

1. Inleiding

«Vertrouwen» is het sleutelbegrip voor de verdere ontwikkeling van de elektronische snelweg. De elektronische snelweg kan alleen tot bloei komen indien er bij burgers en bedrijven voldoende vertrouwen bestaat in de integriteit en betrouwbaarheid van elektronisch verkeer. Dit geldt in het bijzonder voor de verdere ontwikkeling van de elektronische handel. Bedrijven en consumenten zullen alleen warm lopen voor handel op de elektronische snelweg indien ze erop kunnen vertrouwen dat die elektronische snelweg beschikbaar en begaanbaar is. Transacties moeten niet worden onderschept en gewijzigd, de identiteit van koper en verkoper moet buiten kijf staan, de geleverde informatie moet betrouwbaar zijn en als wettig bewijsmiddel kunnen dienen. Zoals de gezamenlijke verklaring van de EU-ministers in Bonn het uitdrukte; «it is crucial to build trust and confidence in Global Information Networks ... by safeguarding the interests of society in general, including producers and consumers, particularly through fair and transparent offers of service».[1]

Een deel van dit vertrouwen hangt samen met de bescherming van de persoonlijke levenssfeer en met de mogelijkheid tot afscherming van bedrijfsgeheimen en intellectuele eigendommen tegen inbreuk. Deze onderwerpen komen elders in de nota aan de orde. Hieronder zal specifiek worden ingegaan op enkele andere aspecten die voor dat maatschappelijke vertrouwen van cruciaal belang zijn: de betrouwbaarheid van de technische infrastructuur en de betrouwbaarheid van het elektronisch maatschappelijk verkeer dat van die technische infrastructuur gebruik maakt. Hoewel beide vormen van betrouwbaarheid in de praktijk vaak samenhangen doordat de juridisch-maatschappelijke betrouwbaarheid van communicatie vaak mede afhangt van de betrouwbaarheid van de technische infrastructuur, is een aparte beschouwing niettemin noodzakelijk. Immers, de aard van de problematiek en de structuur van de verantwoordelijkheden verschillen. Aparte aandacht is er voor de rol van TTPs, «Trusted Third Parties», bij het garanderen van betrouwbaarheid.

2. Technische betrouwbaarheid

Burgers en bedrijven moeten er in de eerste plaats op kunnen vertrouwen dat de nieuwe techniek hen niet in de steek laat en dat het elektronisch berichtenverkeer tenminste even veilig en betrouwbaar is als de traditionele middelen van communicatie. Dat betekent bijvoorbeeld, dat ze erop moeten kunnen vertrouwen dat de elektronische middelen in voldoende mate beschikbaar zijn, dat ze niet al te gevoelig zijn voor storing of sabotage en dat er een stipte en correcte aflevering van informatie plaatsvindt. Het zijn deze randvoorwaarden waaraan moeten worden voldaan voor er sprake kan zijn van enig serieus maatschappelijk verkeer over de elektronische snelweg. Zodra de elektronische snelweg een belangrijke economische en maatschappelijke factor is geworden, is het om sociale en economische redenen van het grootste belang dat deze ongestoord blijft functioneren. De maatschappelijke schade van technische storingen zal dan bijzonder groot zijn. Dit speelt nog sterker wanneer de informatiesamenleving zich zodanig zou ontwikkelen, dat de elektronische media de traditionele media volledig verdringen – het derde niveau van ontwikkeling zoals in Deel I B omschreven.

2.1. Beschikbaarheid van technische middelen

Voor de maatschappelijke acceptatie en het massale gebruik van elektronische communicatie is het belangrijk dat de verschillende

[1] Global Information Networks: Ministerial Conference Bonn 6–8 July 1997.

communicatiemiddelen op zoveel mogelijk plaatsen en tijdstippen toegankelijk en werkzaam zijn. Dit is met name voor het economisch verkeer van groot belang. Alle techniek kan echter falen. De kwaliteit van de techniek bepaalt de levensduur. De gevolgen van falende techniek kunnen worden ondervangen door replicatie van de kritische delen van systemen en netten. Moderne centrales in een telefoonnetwerk en computersystemen in kritische toepassingen zijn dubbel, drievoudig of viervoudig uitgevoerd. De telecommunicatieverbindingen van een aandelenbeurs worden bijvoorbeeld onafhankelijk dubbel uitgevoerd. Onbenutte verwerkingscapaciteit vergroot de betrouwbaarheid als deze bij een calamiteit kan worden ingezet als reservecapaciteit. Een ander soort technische beschikbaarheidsgarantie wordt bereikt door de capaciteit goed af te stemmen op de vraag van de gebruiker.
Voorbeelden van een tekort aan technische middelen om aan de vraag te kunnen voldoen zijn: congestietoon of geen kiestoon bij de telefoon, traag binnenkomen van gegevens van Internet, de trage aflevering van een e-mail of de mailbox niet kunnen openen. Op dit moment is bijvoorbeeld de overbelasting van Internet tijdens Amerikaanse kantooruren een probleem voor verdere groei van elektronische handel. Ook komt het soms voor dat grote delen van Internet plotseling door technische fouten onbereikbaar zijn. Dit gebeurde bijvoorbeeld op 18 juli 1997, toen door een fout van een systeembeheerder bij een Internet-backbone-aanbieder, alle route-servers in de Verenigde Staten de verkeerde elektronische adressen kregen. Hierdoor was bijna 90% van de locaties in de VS urenlang onbereikbaar. Dit soort technische betrouwbaarheidskwesties is in de regel te herleiden tot economische aspecten. De betrouwbaarheid kan worden verhoogd door extra investeringen: extra capaciteit, netwerk-redundantie, reservesystemen, reservekopieën van gegevens, permanent systeembeheer, etcetera.
De overheid bemoeit zich in de meeste westerse landen ook nu al met de betrouwbaarheid en beschikbaarheid van cruciale nutsvoorzieningen, zoals telefonie, elektriciteit energie en water. In hoogontwikkelde samenlevingen is de schade door stroomstoringen of het uitvallen van het telefoonverkeer enorm. Daarom stelt de overheid kwaliteitseisen aan dergelijke nutsvoorzieningen. Dit gebeurt bijvoorbeeld in de vorm van «voorzieningszekerheid», zoals in de Elektriciteitswet. Ook het voorstel voor de nieuwe Telecommunicatiewet gaat uit van functionele eisen van de telecommunicatie-infrastructuur, zoals integriteit, compatibiliteit, volledigheid en ruimtelijke dichtheid. Daarbij is er aparte aandacht voor het ongestoord functioneren van de telecommunicatie in bijzondere omstandigheden. Indien elektronisch verkeer in de toekomst de rol van telefonie en post gaat overnemen, zullen dergelijke maatschappelijke belangen onverkort blijven spelen. Er blijft hier dan ook een taak voor de overheid weggelegd.

2.2. Bescherming tegen inbreuken door technische oorzaken

Gebruikers van de elektronische snelweg moeten er op kunnen vertrouwen dat de berichten die ze versturen, niet verdwijnen of worden verminkt door inbreuken ten gevolge van technisch falen of van onheil van buiten, zoals blikseminslag en stroomstoringen.
Hoewel de bescherming tegen technische inbreuken in eerste instantie een zaak is van de producenten, is het maatschappelijk belang vaak dermate groot dat een stimulerende en ordenende rol van de overheid geboden is (men denke aan de millenium-problematiek). Ook op dit punt gaat de parallel met de meer traditionele communicatiemiddelen op. Het voorstel voor de nieuwe Telecommunicatiewet kent uitgebreide voorschriften die toezien op de kwaliteit van de gebruikte randapparatuur en op hun elektromagnetische compatibiliteit. Deze moeten ook worden toegepast op Internetapplicaties. Daarnaast bieden de algemene

regelingen van het Burgerlijk Wetboek voldoende garanties. Het kabinet stelt voor dit onderwerp over enkele jaren nogmaals te bezien.

2.3. Technisch onomstotelijke vastlegging van systeemgegevens over een communicatie

Voor het economisch en juridisch verkeer is het van groot belang dat gebruikers erop kunnen vertrouwen dat uitgewisselde berichten later als bewijsmiddel kunnen worden gebruikt. Indien men wil dat elektronisch berichtenverkeer in ieder geval gedeeltelijk de plaats inneemt van het papieren verkeer, dan mag er geen twijfel bestaan over de technische gegevens van elektronisch uitgewisselde berichten. Als computersystemen de overdracht van informatie besturen – bijvoorbeeld bij telecommunicatie – dan kunnen deze systemen onder bepaalde voorwaarden met controleerbaar juiste systeemgegevens, zoals datum en tijd van een transmissie, netwerkadressen en dergelijke, registreren wat er precies gebeurt. Deze gegevens leveren bewijsmateriaal waarmee vragen kunnen worden beantwoord rondom aansprakelijkheid van informatie en handelingen. Netwerkadressen zijn nodig voor het routeren van verbindingen en het afleveren van berichten. Voor het leveren van het bewijs van tijdige aflevering van een bericht, of bij de juiste persoon of instantie, is een consistent netwerk-adresseringsstelsel dus een eerste vereiste. Technische condities in de vorm van betrouwbaar geregistreerde systeemgegevens zijn in ieder geval belangrijk. Hieronder vallen bijvoorbeeld onderlinge afspraken tussen informatietechnologische dienstverleners over de technische administratie en de daarvoor vereiste technische en procedurele condities. In beginsel behoort het tot de verantwoordelijkheid van maatschappelijke partijen om bij gerechtelijke procedures zelf zorg te dragen voor wettige bewijsmiddelen. De vraag in hoeverre elektronische uitingen als bewijsmiddel kunnen gelden, is daarom in eerste instantie een vraag die bij de rechter thuis hoort. Ondersteuning door wetgeving met het oog op een verbetering van de mogelijkheden van privaatrechtelijke rechtshandhaving wordt op dit moment niet nodig geacht (zie ook Deel III F).

2.4. Technische duurzaamheid van elektronische documenten

Gebruikers moeten erop kunnen vertrouwen dat hun berichtenverkeer een zekere mate van houdbaarheid heeft. Voor de maatschappelijke betekenis van de elektronische snelweg is het van groot belang dat elektronische berichten kunnen worden bewaard en leesbaar blijven. Het vraagstuk van de digitale duurzaamheid is uiteraard sterk afhankelijk van de gebruikte technologie. Bij elektronisch berichtenverkeer en elektronische opslag van documenten lijken zich thans twee technische betrouwbaarheidsrisico's voor te doen. In de eerste plaats is het nog niet duidelijk in hoeverre de magnetische opslag duurzaam is. In de tweede plaats vormt met name de grote omloopsnelheid van tekstverwerkingsprogramma's en gegevensdragers een groot probleem voor het duurzaam beschikbaar en leesbaar houden van elektronisch vastgelegde gegevens. Zelfs indien de gegevensdragers technisch betrouwbaar blijken, zou bijvoorbeeld software die nodig is om de gegevens te lezen, of de apparatuur die nodig is om de diskette af te spelen, niet meer beschikbaar zijn. Als bijvoorbeeld een authentieke akte wordt vastgelegd op een digitale gegevensdrager, moeten eisen worden gesteld aan de duurzaamheid van het medium. Het document zal misschien na 20 jaar nog leesbaar moeten zijn. Dit betekent dat de gegevensdrager deze houdbaarheid moet hebben. Het computersysteem dat de gegevens kan verwerken moet dan nog beschikbaar zijn. De digitale code waarin de informatie wordt bewaard, moet nog interpreteerbaar zijn. Gezien de snelheid waarmee de informatie- en communica-

tietechnologieën elkaar vandaag opvolgen, zijn deze eisen allerminst vanzelfsprekend.
Het totstandbrengen of stimuleren van voorzieningen die de duurzaamheid van uitingen en documenten bevorderen, behoort thans in zijn algemeenheid niet tot de kerntaken van de overheid. Dit zal rond de elektronische snelweg niet anders zijn. Het opslaan en bewaren van uitingen is in eerste instantie de verantwoordelijkheid van de gebruikers zelf. Dit wordt echter anders, indien met de duurzaamheid van uitingen en documenten een algemeen maatschappelijk belang is gediend. In dat verband kan men denken aan voorzieningen zoals het Kadaster en tal van andere openbare registers, aan authentieke akten, testamenten en andere documenten die de vermogensbetrekkingen en familieverhoudingen tussen rechtssubjecten vastleggen en aan het historisch erfgoed dat is opgeslagen in de vele archieven.[1] In deze gevallen stelt de overheid specifieke eisen aan vorm, aard en duur van de opslag, bijvoorbeeld in de Archiefwet, het Burgerlijk Wetboek en tal van bijzondere wetten.
Van de overheid mag worden verwacht dat zij erop toeziet, dat de maatschappelijke belangen die met de duurzaamheid zijn gediend ook bij een elektronische vormgeving niet in het geding komen. Dit kan verschillende vormen aannemen. De overheid kan soms volstaan met het opleggen van een resultaatsverplichting en alleen in algemene zin eisen dat bepaalde elektronische documenten ook na een bepaald aantal jaren nog in de authentieke vorm zijn te raadplegen. Zij kan ook verder gaan en specifieke eisen stellen aan de opslag, bijvoorbeeld door vormeisen te stellen aan de gebruikte digitale codes of de fysieke eigenschappen van de gegevensdragers, of door op andere manieren te komen tot een standaardisatie van de elektronische opslag van die gegevens die vitaal zijn voor het maatschappelijk verkeer. In ieder geval zal het kabinet bevorderen dat zelfregulering op dit vlak tot stand komt.
Een internationaal vergelijkend stand van zaken-onderzoek naar wettelijke bepalingen waarin duurzaamheidseisen worden gesteld aan het bewaren van in het maatschappelijk verkeer belangrijke (elektronische) documenten, zoals bijvoorbeeld authentieke akten, is opgenomen in de ITER-onderzoeksplanning. In aansluiting daarop vindt een inventarisatie plaats van de wettelijke bepalingen waarin duurzaamheidseisen worden gesteld aan het bewaren van in het maatschappelijke verkeer belangrijke (elektronische) documenten, zoals authentieke akten met het oog op de vaststelling of technologie-afhankelijke normen nodig zijn, wat de doelstelling van de bewaring is en wat daarom de vereiste tijdsduur van de bewaring moet zijn.

3. Juridische betrouwbaarheid

Burgers en bedrijven moeten er op kunnen vertrouwen dat hun onderlinge communicatie op de elektronische snelweg in maatschappelijk en juridisch opzicht betrouwbaar is. Ze moeten er bijvoorbeeld op kunnen vertrouwen, dat informatie juist is, dat degene met wie ze communiceren ook degene is wie deze voorgeeft te zijn, dat aanbiedingen en contracten rechtsgeldig zijn en dat ze, in geval van een conflict, de elektronische informatie in rechte als bewijsmiddel kunnen gebruiken. Een van de oudste taken van een overheid is het scheppen van condities voor een ordelijk en betrouwbaar maatschappelijk en economisch verkeer. Nu een steeds groter deel van dit verkeer zich op de elektronische snelweg afspeelt, rijst de vraag in hoeverre er voor de elektronische omgeving een vergelijkbare taak voor de overheid is weggelegd.

De betrouwbaarheid van de juridische infrastructuur voor het maatschappelijk elektronisch verkeer wordt in deze analyse beschouwd vanuit zes condities die samen betrouwbaar elektronisch maatschappelijk verkeer mogelijk maken:

[1] De duurzaamheid van overheidsinformatie, zoals besluiten, beschikkingen, briefwisselingen, notulen, notas en rekeningen is uiteraard van groot maatschappelijk belang, niet alleen voor historisch onderzoek, maar ook voor politieke en juridische vormen van verantwoording. Deze is reeds het onderwerp van het onderzoeksprogramma Digitale Duurzaamheid, een samenwerkingsverband van het ministerie van BiZa, de Rijksarchiefdienst en een aantal andere betrokkenen en zal hier niet apart aan de orde komen.

1. Transparantie van wat op het beeldscherm zichtbaar is.
2. Kenbaarheid van de bedoelingen van de wederpartij bij elektronische communicatie.
3. Het te goeder trouw zijn van de elektronische wederpartij.
4. Het kunnen onderkennen van handelingsbevoegdheid van de elektronische wederpartij.
5. Het kunnen vaststellen van de echtheid van elektronische documenten.
6. Het kunnen vaststellen van de identiteit van de persoon van de elektronische wederpartij.

Hierbij behoort een kanttekening. Elektronische ontsluiting van openbare registers speelt in dit hoofdstuk een belangrijke rol.De moderne informatietechnologie maakt het mogelijk zoekfuncties uit te oefenen. Bovendien kunnen meerdere digitaal ter beschikking staande openbare registers met elkaar worden vergeleken. Diep op de persoonlijke levenssfeer ingrijpende zoekvragen kunnen dan worden gesteld: bijvoorbeeld hoeveel personen in een bepaalde woonwijk hebben een bestuurdersfunctie in een rechtspersoon (handelsregister), zijn de afgelopen twee jaar meer dan twee keer failliet gegaan (faillissementregister) en wonen in een huis boven een bepaalde prijsklasse (kadaster). Over personen die voldoen aan aldus geformuleerde zoekcriteria kan allerlei informatie worden verkregen, zeker wanneer deze wordt gevoegd bij informatie die op Internet over allerlei personen kan worden verkregen. In besluitvorming over elektronische ontsluiting dient dit privacy-risico steeds te worden meegewogen.

3.1. Transparantie van de beeldschermpresentatie

Gebruikers van de elektronische snelweg moeten erop kunnen vertrouwen dat datgene wat ze te zien krijgen, bijvoorbeeld een document, een elektronische locatie, een e-mailadres of nieuwsgroep, een voorgegeven plaats van verzending, ook echt de werkelijkheid aangeeft. De mogelijkheden om de werkelijkheid anders voor te stellen, zijn in een elektronische omgeving namelijk legio. Op zichzelf zijn deze manipulatiemogelijkheden niet nieuw, maar wel nieuw zijn de enorme schaal waarop dit in een elektronische omgeving kan plaatsvinden, in combinatie met het feit dat het ontdekken moeilijker wordt. Dit kan leiden tot actie van de overheid.
Wat betreft het strafrecht is het onderzoek van belang dat wordt aangekondigd in Deel II, C-3 naar artikel 350a WvSr. Onderzocht moet worden of in de manipulatie van elektronisch overgedragen gegevens een nieuw informatiedelict kan worden gezien[1]. Als er vormen van manipulatie die niet vallen onder traditionele delictsomschrijvingen – misleiding, oplichting, vervalsing en dergelijke – technisch mogelijk blijken te zijn, kunnen hiervoor nieuwe, algemene delictsomschrijvingen worden ontworpen. Deze omschrijvingen zouden dan betrekking moeten hebben op stromende informatie, want voor opgeslagen informatie biedt art. 350a WvSr al zon algemene omschrijving. In de privaatrechtelijke sfeer zijn voor eigen rechtshandhaving voor de burger de gebruikelijke rechtsmiddelen beschikbaar. Voor dit betrouwbaarheidsaspect lijken die toereikend. Preventie van de manipulatie van beeld of geluid – beide moeilijk te ontdekken – is in algemene zin geen taak van de overheid. Dit ligt echter anders als het officiële gegevens betreft, vooral als die van de overheid afkomstig zijn. Ook in de niet-elektronische omgeving zorgt de overheid er al voor dat bijvoorbeeld de geldigheid van identiteitsbewijzen door particulieren kan worden geverifieerd. Het is niet ondenkbaar dat het vraagstuk van betrouwbare communicatie van de overheid er om vraagt dat meer verificatiefaciliteiten in de elektronische omgeving ter beschikking worden gesteld, bijvoorbeeld in de vorm van elektronische identiteitsbewijzen, al dan niet ondersteund door TTP's. Voor

[1] Een internationaal rechtsvergelijkend onderzoek naar bestaan en toepassing van wettelijke strafbepalingen met betrekking tot het manipuleren van webpages (in HTML) tijdens transport is opgenomen in de ITER-onderzoeksplanning 1998.

niet-overheidsgegevens, zoals bij «gironummer-naam-verificatie», ligt dit niet voor de hand.

3.2. Kenbaarheid van de bedoelingen van de wederpartij

De bedoelingen van de wederpartij moeten goed kunnen worden begrepen. Gebruikers van de elektronische snelweg moeten erop kunnen vertrouwen, dat datgene wat hen wordt gepresenteerd, ook als zodanig is bedoeld. Het gaat daarbij bijvoorbeeld om juridische leerstukken, zoals wilsuiting en dwaling. Er moet bescherming bestaan tegen allerlei vormen van communicatie met valse voorwendsels, overigens dat sprake hoeft te zijn van strafbaar gedrag. Men kan hierbij denken aan marktonderzoek met pseudo-verkoop: in plaats van naar meningen te vragen, biedt men een artikel aan duizenden mensen te koop aan. De successcore wordt gerapporteerd en de kooplustigen krijgen een «uitverkocht»-bericht. Vooralsnog lijkt geen nieuwe wetgeving nodig. Het bestaande privaatrecht lijkt voldoende bescherming te bieden. Elektronische colportage is een ander voorbeeld: impulsaankopen onder omstandigheden die dwaling impliceren. In Nederland biedt de Colportagewet echter geen bescherming voor elektronische colportage. Die bescherming zal worden gecreëerd door de implementatie van Richtlijn 97/7/EG betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten. Implementatie in het Burgerlijk Wetboek dient uiterlijk in juni 2000 te zijn voltooid.

3.3. Bona fides, goede trouw, van de wederpartij

Ook goed begrepen bedoelingen kunnen dubbele bodems of misleidingen bevatten. De goede trouw vormt daarom een apart betrouwbaarheids-aspect. Daarbij gaat het niet om misverstanden en onbegrip, zoals in de vorige categorie, maar om welbewuste misleiding van de tegenpartij. De verwachting bestaat dat kwade trouw – bedrog, oplichting – in een elektronische omgeving dermate lastig is te ontdekken is en zoveel bewijsmoeilijkheden oplevert, dat deze op de elektronische snelweg een grote vlucht zal nemen. Dit rechtvaardigt de verwachting, dat op dit punt een appel op de overheid zal worden gedaan. Men bedenke bijvoorbeeld, dat één enkele oplichter in een elektronische omgeving zonder moeite op zon grote schaal kan opereren, dat het elektronisch handelsverkeer kan worden ontwricht. Preventie vergt waarschijnlijk nieuwe detectie- en opsporingstechnieken. Nader onderzoek is nodig naar de technische, maatschappelijke en juridische haalbaarheid van deze technieken. Er is geen behoefte aan nieuwe materiële strafrechtelijke bepalingen. Ter verbetering van de mogelijkheden van strafrechtelijke optreden, streeft het kabinet naar internationale afspraken over de opsporing en vervolging van elektronische vormen van bedrog. Het onderzoek naar de detectie- en opsporingstechnieken kan daarbij een rol spelen. Het kabinet hecht eraan dat er zelfregulering tot stand komt over elektronische pseudokoop en andere vormen van misleiding van consumenten langs elektronische weg. Zij zal de totstandkoming actief bevorderen in overleg met de Consumentenbond en de relevante brancheorganisaties.

3.4. Bevoegd handelen van de wederpartij

Handelen met een onbevoegde wederpartij levert een onvolkomen transactie op. De deelnemer aan het elektronisch verkeer moet er dus van op aan kunnen, dat zijn wederpartij bevoegd is tot de rechtshandeling die hij verricht. Het gaat hier met name om twee categorieën onbevoegden: handelingsonbekwamen en onbevoegde vertegenwoordigers van personen en rechtspersonen.
Handelingsonbekwaamheid, als onderdeel van de bescherming van

minderjarigen en geestelijk of lichamelijk onvermogende personen, is van oudsher een terrein waarop de wetgever voorzieningen treft, zoals publicatievoorschriften, voogdij en curatele. In de elektronische omgeving wordt vooral de kenbaarheid van situaties van handelingsonbekwaamheid problematisch, doordat direct contact doorgaans ontbreekt. In een elektronische omgeving zijn daarom voor preventieve doeleinden nieuwe publicatievormen of signaleringen nodig.[1] Zo zouden de bestaande curateleregisters elektronisch ontsloten moeten worden. Bij omvangrijke of bijzondere transacties kan dan het risico worden gelegd bij de aanbiedende partij, die dient te verifiëren of de wederpartij handelingsbekwaam is.
De bevoegdheid om een natuurlijk persoon of rechtspersoon te vertegenwoordigen, wordt soms door publiekrecht, zoals bijvoorbeeld in de Kieswet, maar meestal door de algemene regels van het privaatrecht bepaald. Dit geldt ook voor de bescherming tegen de gevolgen van onbevoegd handelen. Maar in sommige gevallen heeft de overheid gezorgd voor extra wettelijke voorzieningen, zoals het handelsregister. Voor verificatie van de bevoegdheid een rechtspersoon te vertegenwoordigen, kan de burger het handelsregister van de Kamers van Koophandel raadplegen. Dit register kan in een elektronische omgeving een vergelijkbare functie vervullen. Daartoe dient het echter elektronisch te worden ontsloten. Hierover zijn internationale afspraken, bijvoorbeeld in EU-verband, gewenst.
Op de elektronische snelweg is de wederpartij vaak onbekend en onzichtbaar. De schaal waarop verificatie wordt gewenst en de noodzakelijke snelheid en trefzekerheid daarvan op een elektronische snelweg, is van een andere orde dan in het huidige maatschappelijke verkeer.De overheid zal zorg dragen voor elektronisch toegankelijke verificatieregisters waarmee organisaties, die onderworpen zijn aan een identificatieplicht, of die anderszins een maatschappelijk erkend belang nastreven, op een passende manier de geldigheid van een identiteitsbewijs kunnen controleren. Het moet worden onderzocht welke internationale afspraken hierover, in verband met grensoverschrijdende verificatiebehoeften, wenselijk zijn.

Dit betrouwbaarheidsaspect speelt ook een rol in het bestuursrecht en het strafrecht. Bij een elektronische transactie kan door de verkoper niet meer op grond van zintuiglijke waarnemingen worden vastgesteld of hij zaken doet met een minderjarige en zich dus aan een strafbaar feit schuldig maakt. Voor bedrijven zijn voorzieningen nodig, zodat deze de leeftijd kunnen verifiëren van jeugdige klanten die zij niet kunnen zien. Nader onderzoek is nodig of ontsluiting van openbare registers, dan wel de uitgifte van elektronische identiteitsbewijzen hiertoe maatschappelijk wenselijk en technisch haalbaar is. Bij dit onderzoek wordt de behoefte internationale afspraken in verband met grensoverschrijdende verificatiebehoeften betrokken. De prijsstelling van gegevens in openbare registraties wordt nog onderzocht door het ministerie van Binnenlandse Zaken in het kader van de uitvoering van de Nota toegankelijkheid van overheidsinformatie.

3.5. Echtheid van documenten, berichten en transacties

Men moet in staat zijn om de echtheid van elektronische geuite intenties, verklaringen en documenten te verifiëren. Een waarmerk van echtheid – in de vorm van encryptie via een digitaal certificaat of een digitale handtekening – kan daarvoor garanties geven. Zon waarmerk maakt ook het afleiden van de herkomst mogelijk. Deze technieken zullen op allerlei belangrijke rechtsgebieden van belang zijn. Men denke hierbij bijvoorbeeld aan auteursrecht, elektronische aangiften, geboorteakten, correspondentie en contracten. Met biometrische technieken kunnen fysieke

[1] Een internationaal rechtsvergelijkend onderzoek naar voorzieningen rondom handelings-(on)bekwaamheid op de elektronische snelweg is opgenomen in de ITER-onderzoeksplanning 1998. In dit onderzoek wordt tevens gelet op verschillen in de aard van registers (bijvoorbeeld of een register een positief of negatief karakter heeft).

kenmerken worden gekoppeld aan pincodes of een ander getal, waarmee in veel situaties een beheersbaar anoniem elektronisch maatschappelijk verkeer mogelijk is.
De betekenis van zon waarmerk voor bewijsvoering is enorm. Voor privaatrecht, strafrecht en bestuursrecht geldt de vrije bewijsleer: de rechter kan van geval tot geval bepalen welke bewijskracht hij aan een elektronisch document toekent. Strafrechtelijk bewijs dient daarnaast ook wettig en overtuigend te zijn. Documenten en uitgewisselde berichten moeten daarom later als bewijsmiddel kunnen worden gebruikt. Een waarmerk kan hierbij helpen, hoewel daarnaast ook meestal een bewijsrechtelijk voldoende verbinding naar natuurlijke personen moet kunnen worden gelegd.
Op tal van plaatsen bestaan wettelijke vormvoorschriften voor documenten en transacties. Maar er speelt meer. Voor de echtheid van elektronische documenten en elektronische transacties op specifieke elektronische markten, is ook waarmerking met encryptietechnieken noodzakelijk. Het gebruik van anonieme biometrie op sommige elektronische markten, die nodig kan zijn om de echtheid van personen zonder identificeerbaarheid toch te kunnen garanderen, is hiermee vergelijkbaar. Het is onduidelijk of de ontwikkeling van anonieme biometrie en waarmerking met encryptie door de private sector in voldoende mate de hier beoogde maatschappelijke functie kan realiseren. Het is te overwegen om de overheid deze zorg zelf op zich te laten nemen, of in opdracht te laten verzorgen. Dit laatste bijvoorbeeld voor essentiële overheidstaken, om bijtijds voor dit soort dienstverlening zelf de gewenste normen te stellen. In afwachting van het onderzoek naar de ontwikkeling van elektronische identificatiedocumenten wordt op dit punt geen verdere actie ondernomen.

Tot slot kunnen TTP's natuurlijk een belangrijke rol spelen bij het vaststellen van de echtheid van documenten, berichten en transacties.

3.6. Identificeerbaarheid van natuurlijke personen

Door middel van encryptie en andere technieken is een document of transactie te waarmerken als authentiek, maar te identiteit van het rechtssubject valt niet altijd vast te stellen. Voor een betrouwbaar economisch verkeer is in veel gevallen nodig dat de ware identiteit van een partij kan worden vastgesteld. In dit verband blijkt de belangstelling voor biometrische persoonsverificatie de laatste jaren te groeien. Anders dan bijvoorbeeld met een PIN-code, legt een biometrisch persoonskenmerk – vingerafdruk, dynamische handtekening of handpalmgeografie – een directe, niet overdraagbare verbinding met een natuurlijke persoon. Een biometrisch kenmerk kan men ook niet vergeten of verliezen. De PIN-code daarentegen legt alleen een administratieve verbinding, deze kan worden vergeten en verloren en is te gemakkelijk overdraagbaar aan derden.
Biometrische persoonsverificatie kan in een elektronische omgeving voorzien in de behoefte de identiteit van natuurlijke personen beter vast te stellen. Het belang voor de bewijsvoering is groot. Ook voor persoonsverificatie geldt in alle rechtsgebieden een vrije bewijsleer: de rechter kan van geval tot geval bepalen welke bewijskracht hij toekent aan een persoonsverificatie, waarbij gebezigde procedures en technieken van belang zijn. Wat het waarmerk doet voor documenten, berichten en transacties, doet een biometrische persoonsverificatie voor personen. Biometrische persoonsverificatie is ook van belang in de strijd tegen elektronisch witwassen van criminele vermogens, of tegen elektronische terreur, zoals «electronic stalking». Preventie van meervoudige elektronische identiteiten en elektronische dubbelgangers zal van de overheid nieuwe maatregelen vragen. Daarbij zal de mogelijkheid de ware identiteit

van een natuurlijk persoon vast te stellen en deze vervolgens met biometrie te verifiëren in een elektronische omgeving een belangrijke rol spelen.
Organisaties die sectorale nummers, chipcards, pseudo-identiteiten, sleutels of passwords aan personen uitgeven, mogen van die personen een deugdelijke legitimatie verlangen. Dat kan worden gerealiseerd door de Wet op de identificatieplicht uit te breiden met het oog op enkele elektronische markten, analoog aan de reeds bestaande regeling van de uitgifte van het sofi-nummer door de Belastingdienst. Bij twijfelgevallen moet de mogelijkheid bestaan een grondiger onderzoek te laten plaatsvinden naar iemands juiste identiteit. Bij belangrijke overheidstaken zou de overheid deze zaken, met het oog de gewenste kwaliteit en betrouwbaarheid, zelf ter hand moeten nemen. Het personaliseren van chipcards die persoonlijk toegang geven tot de elektronische snelweg, zoals bijvoorbeeld GSM-kaarten, dient onder de werking van de Wet op de identificatieplicht te worden gebracht. Zie hiervoor het voorstel in Deel III C.
Voorts is wenselijk dat ter verbetering van de identificatiemogelijkheden onderzoek plaatsvindt naar de ontwikkeling van elektronische equivalenten voor de schriftelijke en bij de wet erkende, identificatiedocumenten (zie ook hiervoor III C).

Recent heeft het kabinet besloten tot de ontwikkeling van een nieuwe generatie reisdocumenten. In dit kader zal onder meer de wenselijkheid en toepasbaarheid van de opname van aanvullende biometrische kenmerken op de reisdocumenten worden onderzocht. De ontwikkelingen met de burgerservicekaart zullen positief worden gevolgd waarbij te zijner tijd als de beleidsmatige keuzes met betrekking tot de nieuwe generatie reisdocumenten duidelijk zijn, zal worden bezien of integratie van de burgerservicekaart met reisdocumenten wenselijk en mogelijk is.

4. TTP's

Onder verantwoordelijkheid van de Ministers van Verkeer en Waterstaat en van Economische Zaken wordt thans onderzoek gedaan naar Trusted Third Parties (TTP's). Dit onderzoek mondt uit in een notitie aan de Tweede Kamer, die in het voorjaar van 1998 valt te verwachten. Die notitie gaat vooral in op de technische inrichting en infrastructuur van TTP-diensten.
In deze nota staat de rol die TTP's moeten gaan spelen in het elektronisch rechtsverkeer centraal.

TTP's zijn instanties die een intermediaire rol vervullen in het elektronische berichten- en geldverkeer. In het elektronische verkeer kunnen partijen behoefte hebben aan extra garanties omtrent de betrouwbaarheid van de berichtenstromen. Vaak kan de verificatie van deze betrouwbaarheid alleen langs elektronische weg kan plaatsvinden, ongeveer zoals accountants de betrouwbaarheid van financiële rapportage garanderen en notarissen die van contracten. Dit is soms het geval, omdat de partijen zich op grote afstand bevinden en niet op korte termijn persoonlijk met elkaar in contact kunnen treden. In die gevallen kan het nuttig zijn wanneer er instellingen zijn die de betrouwbaarheid van het elektronische berichtenverkeer kunnen garanderen, een rol die in het elektronische verkeer in toenemende mate wordt vervuld door TTP's.

TTP's leveren de volgende kerndiensten:
- Het verzekeren van de integriteit van een bestand of boodschap: is de boodschap die de lezer onder ogen krijgt identiek aan de boodschap die verzonden is?

- Het vaststellen van de identiteit van een partij: staan partijen werkelijk in contact met diegene met wie zij menen in contact te staan?
- Het digitaal verwerken van contracten met een digitale handtekening: is een contract ondertekend – gezien en akkoord verklaard?
- Time-stamping: is een bericht verzonden of opgeslagen op de tijd waarop een partij zegt dat dit gebeurd is?

Naast deze kerndiensten, kunnen TTP's nog andere diensten uitvoeren, zoals het maken of beheren van back-up bestanden, of het uitgeven of beheren van encryptie-sleutels. TTP's kunnen in potentie nog een andere functie vervullen: behulpzaam zijn bij «key recovery» of «key escrow», voor via de TTP verzonden geëncrypteerde berichten, waardoor toegang tot bestanden en boodschappen door inlichtingen- en opsporings-autoriteiten gewaarborgd is. Deze vorm van TTP, instellingen die niet alleen een functie hebben bij het vergroten van de betrouwbaarheid van elektronische communicatie, maar die ook een rol hebben in de strafrechtelijke handhaving, is op zichzelf niet zo bijzonder. Immers, onder voorwaarden zijn ook huidige instellingen, die vertrouwelijke gegevens van cliënten onder hun hoede hebben, in bepaalde gevallen verplicht mee te werken aan opsporingsonderzoek. Deze functie van TTP's komt in het hoofdstuk rechtshandhaving aan de orde.

In het buitenland en in de academische literatuur gaat men er meestal vanuit dat TTP's door de overheid worden gecertificeerd. Het kan hierbij gaan om bestaande instellingen die de elektronische dienst in hun totale aanbod opnemen – accountantskantoren, advocatenkantoren, banken, of notarissen - of om gespecialiseerde nieuwe instellingen. Om de rol als bona fide aanbieder van intermediaire diensten te kunnen vervullen, moeten aan een TTP een reeks van eisen worden gesteld. Deze hebben onder andere betrekking op:

- *De technische inrichting van de computersystemen:* behalve dat ze betrouwbaar moeten zijn, moeten computersystemen van TTP's vooral transparantie hebben, omdat de werking aan nauwgezette controles onderworpen moet kunnen worden.
- *De te gebruiken software:* voor de software geldt om dezelfde reden een hoge mate van vereiste transparantie.
- *Opleiding van personeel:* te denken valt aan opleidingseisen en registratie, vergelijkbaar aan die bij accountants en EDP-auditors. Om flexibiliteit te bewaren – TTP's kunnen in de toekomst ook andere diensten gaan verrichten dan nu voor de hand lijken te liggen en ook de te gebruiken systemen kunnen sterk veranderen – is het aan te bevelen ook een registratie van bona fide en professionele informatici open te stellen. Dit op basis van het huidige systeem van Register Informatici.
- *Betrouwbaarheid van personeel:* zij die in het verleden betrokken zijn geweest bij vermogensmisdrijven en fraude, zouden geen cruciale posten bij een TTP mogen bezetten.
- *Bewaartijd van gegevens en systemen:* om controles achteraf mogelijk te maken, bijvoorbeeld bij geschillen tussen cliënten van TTP's is een bewaartijd – die in verband staat tot de soort dienst – van gegevens of het bijhouden van log-bestanden een vereiste.
- *Toegankelijkheid van systemen:* binnen de TTP moeten systemen niet zonder meer voor iedereen openstaan.
- *Het beheer van gegevens van een op te heffen TTP:* in principe moeten de gegevens van een TTP bij opheffing of bedrijfsbeëindiging – net als bij notarissen – bij een andere TTP, of bij een apart register kunnen worden ondergebracht.

In deze eisen kan worden voorzien door middel van zelfregulering, die wordt ondersteund door een stelsel van overheidstoezicht. Daarbij kan worden voortgebouwd op ervaringen die bij andere intermediaire

instanties zijn opgedaan, zoals de accountancy en het notariaat. In de evengenoemde notitie van de Ministers van Verkeer en Waterstaat en Economische Zaken zal aan dit voornemen nader vorm worden gegeven. Daarnaast kan, overeenkomstig deel II C van deze nota, een juridisch kader voor TTP's ondersteunend werken. Bovendien wordt, overeenkomstig Deel III F van de nota, bewijskracht verleend aan door bepaalde TTPs vastgelegde elektronische informatie.

5. Conclusies en voorstellen

5.1. Technische betrouwbaarheid

- De verdere ontwikkeling van een betrouwbare technische infrastructuur is niet à priori een taak van de overheid. Het is de verantwoordelijkheid van de gebruiker zelf om zich al dan niet van elektronische communicatie te bedienen. Risico van en aansprakelijkheid voor falen van dit middel kunnen niet zomaar op anderen – de overheid – worden afgewenteld.
- Dit zou anders kunnen worden wanneer de elektronische snelweg een niveau van ontwikkeling zou bereiken, waarbij burgers en bedrijven daarzonder niet goed kunnen functioneren (het niveau van verdringing als bedoeld in Deel I B van de nota). Dan kan de technische betrouwbaarheid niet uitsluitend aan de markt worden overgelaten.
- Aanpassing van de regelgeving op het punt van de bescherming tegen inbreuken door technische oorzaken is op dit moment nog niet aan de orde. Vooralsnog bieden de voorzieningen in het ontwerp voor de Telecommunicatiewet en de regelingen van het Burgerlijk Wetboek voldoende garanties. Het kabinet stelt voor om dit onderwerp over enige jaren nog eens te bezien.
- Het kabinet hecht er belang aan, dat zelfregulering tot stand komt omtrent de duurzaamheid van belangrijke documenten in het maatschappelijk verkeer. Het kabinet zal de totstandkoming van die zelfregulering actief bevorderen.
- Er vindt een inventarisatie plaats van de wettelijke bepalingen waarin duurzaamheidseisen worden gesteld aan het bewaren van in het maatschappelijk verkeer belangrijke (elektronische) documenten, zoals authentieke akten met het oog op de vaststelling of technologieafhankelijke normen nodig zijn, wat de doelstelling van de bewaring is en wat daarom de vereiste tijdsduur van de bewaring moet zijn, in aansluiting op een internationaal vergelijkend onderzoek dat is opgenomen in de ITER-onderzoeksplanning.

5.2. Juridische betrouwbaarheid

- De algemene, door het burgerlijk recht geboden infrastructuur is voor het elektronisch handelsverkeer doorgaans geschikt en toereikend. In de meeste gevallen geldt ook hier als hoofdregel, dat wie zich bedient van een middel, de risicos daarvan zelf moet dragen.
- Bij communicatie met de overheid zelf is dit minder het geval. In dat geval moet de overheid eisen stellen aan het handelsverkeer, of de verhouding tussen overheid en burger regelen.
- Onderzocht wordt of een nieuw informatiedelict kan worden gezien in de manipulatie van de elektronische overdracht van gegevens naast, of in aanvulling op, art 350a Sr. (zie ook Deel II C-3).
- Het kabinet hecht eraan dat er zelfregulering tot stand komt over elektronische pseudokoop en andere vormen van misleiding van consumenten langs elektronische weg. Zij zal de totstandkoming actief bevorderen in overleg met de Consumentenbond en de relevante brancheorganisaties.
- Nader onderzoek is nodig naar de technische en maatschappelijke

haalbaarheid van detectietechnieken voor de preventie van elektronische vormen van bedrog. Het kabinet streeft naar internationale afspraken over de opsporing en vervolging van elektronische vormen van bedrog.
- De overheid zal zorg dragen voor elektronisch toegankelijke verificatieregisters waarmee organisaties, die onderworpen zijn aan een identificatieplicht, of die anderszins een maatschappelijk erkend belang nastreven, op een passende manier de geldigheid van een identiteitsbewijs kunnen controleren. Het moet worden onderzocht welke internationale afspraken hierover, in verband met grensoverschrijdende verificatiebehoeften, wenselijk zijn.
- Nader onderzoek is nodig of en hoe openbare registers elektronisch toegankelijk kunnen worden gemaakt voor de uitvoering van wettelijke verplichtingen, zoals bijvoorbeeld het verbod bepaalde transacties aan te gaan met minderjarigen. Bij dit onderzoek wordt de behoeft aan internationale afspraken in verband met grensoverschrijdende verificatiebehoeften betrokken.
- Het kabinet zal bevorderen dat de bestaande curateleregisters elektronisch worden ontsloten.
- Het kabinet zal de elektronisch ontsluiting van de bestaande Nederlandse en EU-handelsregisters bevorderen.
- Het verdient overweging om de overheid de taak te geven om de uitgifte te verzorgen van biometrisch beveiligde elektronische identiteitsbewijzen. Uitvoering van dit voornemen vindt plaats binnen het kader van het project. Nieuwe generatie reisdocumenten, waarover de staatssecretaris van Binnenlandse Zaken de Tweede Kamer in januari 1998 heeft geïnformeerd.
- Het kabinet staat positief tegenover de experimentele ontwikkeling van biometrisch beveiligde burgerservicekaarten.
- Onderzoek vindt plaats naar de ontwikkeling van elektronische equivalenten voor de schriftelijke en bij de wet erkende, identificatiedocumenten (zie Deel III C).
- Deel III C doet een voorstel tot uitbreiding van de Wet op de identificatieplicht, met het oog op het personaliseren van chipcards en andere elektronische identiteitsbewijzen die een strikt persoonlijke toegang geven tot de elektronische snelweg. Dit voorstel dient mede het belang van de betrouwbaarheid.

5.3. TTP's

- Bij het garanderen van de juridische betrouwbaarheid van het elektronisch maatschappelijk verkeer zal een belangrijke rol zijn weggelegd voor TTP's.
- Regeling van de activiteiten van TTP's kan door middel van zelfregulering, die wordt ondersteund door overheidstoezicht. Daarbij kan worden voortgebouwd op ervaringen die zijn opgedaan bij andere intermediaire instanties, zoals de accountancy en het notariaat. In de evengenoemde notitie van de Ministers van Verkeer en Waterstaat en Economische Zaken zal aan dit voornemen nader vorm worden gegeven.

E. MARKTEN

1. Inleiding

De elektronische snelweg is meer dan een web van technische koppelingen en verbindingen. De informatiesamenleving is ook een geheel van informatie- en communicatiemarkten[1]. Er zijn drie redenen om deze markten aan een nadere beschouwing te onderwerpen.
In de eerste plaats is er het vraagstuk van een goede ordening en werking van die markten. Dit is vanouds een overheidsdoel. De vraag is echter in hoeverre de markten van informatie- en communicatie afwijken van andere markten en vragen om bijzondere overheidsmaatregelen in de sfeer van mededinging.
In de tweede plaats: voor burgers en bedrijven die informatiediensten en producten willen afnemen, is niet alleen de werking van de markt, maar ook de uitkomst van die marktwerking van belang. In de sfeer van telecommunicatie en informatie is er daarom vanouds aandacht van de overheid voor de vraag of burgers voldoende toegang kunnen krijgen tot de producten en diensten die op die markt worden aangeboden. Dat is het tweede onderwerp dat hieronder aan de orde komt.
In de derde plaats: één van de bijzondere aspecten van deze markten is dat informatie de handelswaar vormt. In een liberale democratie heeft de overheid de bijzondere taak om de inhoud van informatie in de gaten te houden. Artikel 22, derde lid, van de Grondwet draagt haar enerzijds op om voorwaarden te scheppen voor maatschappelijke en culturele ontplooiing, terwijl zij anderzijds ook tot taak heeft op te treden tegen schadelijke of agressieve vormen van informatie of meningsuiting. Deze dubbele taak vormt het derde onderwerp.

2. Mededinging en informatiemarkten

Vrije toetreding tot markten, vrije concurrentie en weinig belemmerende regels zijn op het gebied van de marktwerking belangrijke uitgangspunten van het regeringsbeleid De invoering van de nieuwe Mededingingswet is de voornaamste maatregel op dit terrein geweest. De belangrijkste elementen van het nieuwe mededingingsregime worden besproken besproken in Deel II C-4.
Uit de nieuwe wet blijkt dat het stimuleren van marktwerking niet betekent dat marktpartijen ongehinderd hun gang kunnen gaan. Er zijn regels en er is een instantie (NMA) die toeziet op de naleving daarvan. De wijze waarop het kabinet markten tegemoet treedt, past goed in de eerder beschreven trend waarbij de overheid zich minder richt op zelf presteren en zelf sturen, maar zich concentreert op ordening.
Het principe van vrije mededinging geldt vanzelfsprekend ook voor informatie- en communicatiemarkten – zoals ook blijkt uit het NAP. Eén van de centrale thema's in het NAP, is de liberalisering van de markt voor de elektronische dienstverlening. Als algemeen uitgangspunt kan hier gelden dat waar informatiemarkten niet wezenlijk anders zijn dan de andere markten, de normale mededingingsregels en het normale mededingingsinstrumentarium voldoende moeten zijn om een behoorlijke marktwerking te garanderen. Op een aantal punten zijn de moderne informatie- en telecommunicatiemarkten afwijkend van de reguliere markten. Deze zijn: technologische turbulentie, het grensoverschrijdend karakter, het belang van technische interconnectie en het veelvuldig voorkomen van cross-ownership.
Een vijfde element, de overgang van een monopolie-situatie naar een open markt, blijft hier verder buiten beschouwing.

[1] Deze gedachte is eerder naar voren gebracht door A.W. Koers, *Regulering van het Internet,* 1997, pagina 43.

2.1. Technologische turbulentie

Veel informatie- en communicatiemarkten zijn relatief jong en sterk in ontwikkeling. Het is op dit moment nog niet duidelijk of de regels van de nieuwe Mededingingswet en de Telecommunicatiewet voldoende adequaat zijn om de orde op de informatie- en communicatiemarkten gedurende langere termijn te verzekeren. Het is bijzonder lastig om burgers en bedrijven voldoende zekerheid te bieden omtrent hun rechten en plichten en om tegelijkertijd de regelgeving zodanig technologie-onafhankelijk te maken dat deze duurzaam is.
Een hoge mate van turbulentie vraagt daarom om een actieve rol van de overheid, bijvoorbeeld door toezicht te houden op de markt. De voortdurende technologische verandering op de informatie- en telecommunicatiemarkten vraagt echter om een hoge mate van specialisatie bij de toezichthouder. Zolang de informatie- en communicatiemarkten turbulent en onvoorspelbaar zijn, blijft specifiek toezicht raadzaam, bijvoorbeeld door de OPTA. Het kabinet is van plan om de ontwikkelingen op de markten en die van de activiteiten van de NMA en de OPTA regelmatig te beoordelen. Hierbij kunnen de conclusies en uitgangspunten van het MDW-rapport over «Zicht op toezicht» een belangrijk kader vormen.

2.2. Grensoverschrijdend karakter

Informatiemarkten zijn vooral internationale markten. Voor handhaving van mededingingsregels dreigt hier een gevaar: overtreders van mededingingsregels kunnen zich buiten de eigen rechtsmacht, of zich binnen verscheidene rechtsmachten bevinden – zie hiervoor ook Deel III B van de nota. De Europese Commissie handhaaft mededingingsregels op het niveau van de Europese Unie. Ook is er de laatste jaren in de gehele Europese Unie sprake van convergentie van nationale mededingingsregels.
Lastiger is het wanneer aanbieders zich buiten de EU bevinden. Dit zal zich in de toekomst, door de verdere ontwikkeling van Internet en elektronische handel, in toenemende mate voordoen. Voor een deel is dit een algemeen probleem van internationalisering en rechtsmacht, beschreven in Deel III B. In aanvulling hierop zijn nog twee handhavingsstrategieën specifiek behulpzaam op het terrein van de internationale mededinging:

- Zelfhulp: het toepassen van eigen regels op overtreders die zich buiten de rechtsmacht bevinden, maar wier gedrag concurrentiebeperkend werkt in Nederland of de EU. Het is natuurlijk niet altijd mogelijk om rechtsmacht te verkrijgen over een aanbieder die zich elders bevindt, maar het is wel mogelijk bijvoorbeeld diens producten te weren. De EU heeft met deze strategie bij de voor de Europese vliegtuigbouw bedreigende fusie van Boeing en Lockheed gedreigd.
- Positieve samenwerking (positive comity): een land vraagt de mededingingsautoriteiten in een ander land om een onderzoek in te stellen naar een overtreder – en eventueel tot maatregelen over te gaan – wanneer de overtreding van mededingingsregels beide landen schaadt, maar de overtreder zich in het andere land bevindt.

Een aanbeveling van de OESO uit 1967 en een overeenkomst tussen de EU en de VS in 1991 vormen een basis voor deze beide strategieën. Het kabinet hecht belang aan de ontwikkeling van deze en andere strategieën en zal stappen ondernemen om te komen tot nadere internationale afspraken die de samenwerking tussen mededingingsautoriteiten bevorderen. Gegeven het internationale karakter van de informatie- en communicatiemarkten zijn deze strategieën alleen zinvol indien zij op EU-niveau worden ingezet.

2.3. Technische koppelingen

Informatie- en communicatiemarkten worden gekenmerkt door een technisch complexe infrastructuur. Technische koppelvlakken – «interfaces» – mogen de werking van de markten niet hinderen. Verschillende soorten koppelingen zijn van belang voor de transparantie van de markten: de koppeling van telecommunicatienetten (interconnectie), de koppeling van randapparatuur aan telecommunicatienetten, de koppeling tussen verschillende elementen van eenzelfde netwerk en de koppeling van de computers van dienstenaanbieders aan telecommunicatienetten. Voor een goede marktwerking op dit vlak is standaardisatie van essentieel belang. De marktpartijen moeten kunnen beschikken over sterke technische standaards. Het ontbreken hiervan kan leiden tot het ontstaan van economische machtsblokken: enkele zeer grote bedrijven die de wereldmarkt als monopolist bedienen. Als echter iedereen over dezelfde standaarden kan beschikken, zonder dat enige partij aan dat wijdverspreide gebruik een voordeel kan ontlenen, hebben deze juist een faciliterende rol.
De overheid kan de ontwikkeling van sterke standaards langs verschillende wegen bevorderen:

- Deelname aan, of stimuleren van standaardisatie-organisaties. De overheid kan stimuleren dat standaardisatie via zelfregulering tot stand komt. Veel standaarden hebben geen wettelijke basis, maar worden vastgesteld door normalisatie-instituten en organisaties waar de voornaamste partijen bijeenkomen, zoals bijvoorbeeld ISO, ETSI, ITU-T. Overheden spelen daarbij een stimulerende rol. Dergelijke vormen van zelfregulering mogen er niet toe leiden dat dominante marktpartijen hun positie misbruiken ten nadele van kleinere marktpartijen of consumenten.
- De Paradorstrategie[1]: de overheid kan allereerst trachten zelf – als grootgebruiker van informatie en communicatietechnologie – een standaard op te leggen aan aanbieders van ICT-producten en -diensten, in de hoop dat deze als algemene standaard zal gaan gelden.
- Dwanglicenties: technische macht kan de vorm hebben van een exclusief recht, het octrooirecht.
- De octrooihouder kan commerciële exploitatie van zijn uitvinding verbieden. Wanneer echter een octrooi van groot economisch belang is, kan de Minister van Economische Zaken een dwanglicentie uitvaardigen. In het verleden is deze maatregel zelden toegepast, maar wanneer standaarden steeds belangrijker worden, kan het belangrijk zijn een instrument voor gedwongen medewerking of samenwerking achter de hand te hebben. Overigens kan iedere belanghebbende bij de Octrooiraad of de rechter een verzoek tot een dwanglicentie doen. Het initiatief tot gebruik van dit instrument hoeft dus niet bij de overheid alleen te liggen.
- Toepassen mededingingsregels bij misbruik van octrooirecht door een economisch machtige partij. Dit kan een belangrijk instrument zijn om het misbruik op te heffen van standaarden die door octrooi zijn beschermd.
- Verplichtingen voor marktpartijen: de Telecommunicatiewet zal een regime kennen waarbij een exploitant van een netwerkdienst zijn netwerk op niet discriminerende wijze en tegen een transparant en op kosten georiënteerd uitgesplitst tarief moet hanteren. Ook voor andere markten waar interconnectie een rol speelt, kan een dergelijk regime van kracht worden.
- Wettelijk voorschrijven van een standaard: de meest vergaande stap is het door de overheid rechtstreeks voorschrijven van een wettelijke standaard. Dit is bijvoorbeeld gebeurd met de GSM-standaard voor

[1] Parador is een keten van Staatshotels in Spanje. Na de oorlog koos de Spaanse overheid ervoor niet in wetgeving kwaliteitscriteria voor hotels vast te leggen (teneinde daarmee het toerisme te bevorderen), maar zelf een aantal hotels te beginnen die aan hoge kwaliteitscriteria voldoen. De verwachting was dat andere hotels zich aan die criteria zouden meten. Die verwachting kwam uit.

mobiele telefonie. Dit zal in de praktijk zoveel mogelijk in internationaal verband moeten gebeuren.

Een verdere afweging van al deze maatregelen leidt tot het volgende:
- Standaardisatie komt bij voorkeur tot stand door zelfregulering en via internationale standaardisatie-organisaties. Het kabinet zal de totstandkoming hiervan actief bevorderen. Zelfregulering zal niet mogen leiden tot misbruik van dominante marktposities.
- Dwanglicenties en de toepassing van mededingsregels kunnen bij misbruik van octrooirecht een interessant sluitstuk zijn. De toepassing hiervan wordt nader onderzocht.
- Onderzocht wordt of het zinvol is het interconnectie-regime uit de Telecommunicatiewet op andere informatiemarkten toe te passen.
- Het wettelijk voorschrijven van standaarden heeft geen voorkeur.

2.4. Cross-ownerships

Op sommige informatiemarkten komt «cross-ownership» veelvuldig voor. Bedrijven kopen deelnemingen in elkaar, of richten gezamenlijk nieuwe bedrijven op. Zo kunnen uiterst ingewikkelde conglomeraten ontstaan, die slechts in een aantal handen verkeren en die ook weinig transparant zijn. Op het oog bestaat wel concurrentie, maar de beslissingsmacht is bij een dergelijk conglomeraat van rechtspersonen in slechts enkele handen.
In Nederland is op dit terrein thans nog sprake van minimale wetgeving, in tegenstelling tot in sommige andere Europese landen. Het Verenigd Koninkrijk kent bijvoorbeeld een uitgewerkt regime. Mogelijk zouden de ontwikkelingen op het terrein van het cross-ownership kunnen leiden tot monopolisering van de informatievoorziening. In de Mediawet is wel een zogenaamde Murdoch-bepaling (artikel 82f) opgenomen. Deze bepaling moet machtsconcentratie bij één commerciële ondernemer voorkomen. Nadere regelgeving voor andere informatiemarkten is op dit moment niet gewenst. De Medededingingswet vormt hiervoor voldoende basis. Daar komt nog bij dat op de relatief kleine Nederlandse markt niet altijd plaats is voor meer aanbieders. Er moet wel voor worden gezorgd dat een monopolist niet alle informatiestromen beheert. Van belang is dan ook het onderzoek naar cross-ownership in de mediasector, dat door de ministers van OCW en van Enomische Zaken wordt verricht[1].

3. Toegankelijkheid

Marktwerking is een belangrijk uitgangspunt van het regeringsbeleid, maar het is geen middel voor alle kwalen. Lang niet alle maatschappelijke belangen zijn gediend met het proces van vraag en aanbod. In sommige gevallen kan de markt een bepaalde dienst of product wel leveren, maar alleen tegen een hoge prijs. Hierdoor kan bijvoorbeeld een deel van de burgers geen toegang krijgen tot een bepaald product of een bepaalde voorziening. Ook het functioneren van de wetenschap is gebaat bij een zo groot mogelijke toegang tot informatie.
Toegankelijkheid van informatie en communicatiekanalen is een zo groot maatschappelijk belang dat dit niet altijd aan de markt kan worden overgelaten. In het kader van het overheidsbeleid ten behoeve van een brede toegankelijkheid kunnen een aantal redenen tot interventie worden onderscheiden:
- Het medium is onontbeerlijk voor goed maatschappelijk functioneren van de burger. In het algemeen moet de burger in staat zijn om sociale contacten aan te gaan en te onderhouden met andere burgers en bedrijven, kennis te nemen van informatie en te communiceren met overheidsfunctionarissen en andere maatschappelijke instellingen.
- Het medium kent een schaarste probleem – bijvoorbeeld beperkte

[1] Dit onderzoek vloeit voort uit een motie die tijdens de behandeling van het wetsvoorstel Liberalisering van de Mediawet in de Tweede Kamer is aangenomen, TK 24 808.

frequenties – en de overheid ziet toe op de verdeling van schaarse bandbreedte of zendtijd.
- De overheid tracht een vliegwiel-effect teweeg te brengen. Naarmate meer mensen gebruik maken van een medium wordt dit succesvoller en goedkoper en kan het bijdragen aan economische groei.

De vraag rijst in hoeverre deze overwegingen ook aanleiding zouden kunnen geven tot een inzet van juridisch instrumentarium. Die vraag wordt beantwoord aan de hand van de veranderingen in de telefonie en aan de hand van Internet, als voorbeeld van een geheel nieuw medium.

3.1. Veranderingen in de telefonie

De gedachtegang dat toegang tot telefonie een voorwaarde is voor maatschappelijk functioneren van burgers heeft in het verleden geleid tot twee vragen:
- Hoe kan toegang tot de infrastructuur worden verzekerd? In het bijzonder daar waar gezien de geografie of demografie van een gebied kostendekkende aanleg van infrastructuren niet mogelijk was.
- In hoeverre en hoe, moet de toegang tot informatiediensten van burgers met een laag inkomen worden verzekerd?

Toegang tot de infrastructuur, met name in geografisch of demografisch onaantrekkelijke gebieden, is thans geen reëel probleem meer. Het vaste net heeft een dekking van 99% en daar waar het vaste net geen oplossing biedt, zijn inmiddels andere technische voorzieningen mogelijk, zoals radioverbindingen en GSM. Als er toch nog knelpunten bestaan, kunnen deze worden weggenomen door de verplichting tot universele dienstverlening voor spraaktelefonie, zoals voorzien in artikel 9.1 van de Telecommunicatiewet. De lagere kosten van telecommunicatie – door het beschikbaar komen van meer bandbreedte – maken ook het probleem van de kosten van toegang minder belangrijk. Er zal echter altijd een kleine groep blijven bestaan die niet zonder meer toegang heeft tot telefoonvoorzieningen. Zonodig zouden die burgers direct kunnen worden gesubsidieerd, bijvoorbeeld via de Bijstandswet.
Een belangrijke nieuwe vraag wordt opgeworpen door de komst van «content»-telefoondiensten. Dit zijn zogeheten toegevoegde waardediensten, zoals 06-nummers voor «hapklare» informatie – beursinfo-lijn, file-lijn, ANP-nieuwslijn, sexlijnen, voice mail en dergelijke – waarvan de gesprekskosten zeer hoog kunnen zijn. Het aantal content-telefoondiensten is groeiende. Soms gaan bedrijven en instellingen er toe over om diensten, die tevoren nog tegen gewone gesprekskosten beschikbaar waren, alleen nog aan te bieden via nummers die rond de gulden per minuut kosten. Het is mogelijk dat dit slechts een tijdelijk verschijnsel is. Veel diensten die nu per telefoon worden aangeboden zouden bijvoorbeeld uiteindelijk Internet-diensten kunnen worden. Het is ook mogelijk dat de gesprekskosten weer dalen zodra de initiële investeringen zijn terugverdiend. Daar waar dit niet zo is en de gesprekskosten dus hoog blijven, én de dienst wordt aangemerkt als een voor de burger essentiële dienst, bijvoorbeeld: een rechtshulpnummer, ligt een toegangsprobleem. Het verschaffen van toegang tot diensten die voor bepaalde burgers te duur zijn is echter niet een nieuw probleem: subsidiëring, hetzij van de dienst, hetzij van de burger, kan dit probleem oplossen. In het uiterste geval is ook het regime van art. 9.1 van de nieuwe Telecommunicatiewet beschikbaar. Schaarste en het teweeg brengen van een vliegwieleffect, zijn bij telefonie geen relevante interventiegronden.

3.2. Internet

Tot op heden is er geen regelgeving, gericht op de toegankelijkheid van Internet. De overheid zou kunnen besluiten dat zij een rol heeft bij het breed toegankelijk maken van Internet indien één of meer van de

traditionele redenen tot interventie bij informatiemedia ook voor Internet blijken op te gaan.

3.2.1. Maatschappelijk functioneren van de burger

Op dit moment leidt het ontbreken van toegang tot Internet nog niet tot vermindering van de kwaliteit van het maatschappelijk functioneren. De belangrijkste media waarmee sociale contacten worden onderhouden en die een technische infrastructuur vergen, zijn thans nog steeds de telefoon en de post. Slechts een minderheid van de Nederlandse huishoudens heeft een Internetaansluiting. En zelfs in die huishoudens speelt de telefoon als technisch communicatiemiddel nog steeds de belangrijkste rol. Wel neemt het aantal Internetaansluitingen toe. Daarnaast is nog een trend waar te nemen in het gebruik van Internet: contact per e-mail is een belangrijke vorm van communicatie aan het worden. Telefoon en postbezorging zullen voorlopig echter blijven bestaan, zodat ook voor burgers die geen toegang tot e-mail hebben alternatieve informatiekanalen aanwezig zijn. Indien Internet en e-mail echter de dominante communicatiekanalen in de samenleving worden en de bestaande communicatiemiddelen verdringen, is een actief toegangsbeleid geboden. Een andere wijze waarop de burger in zijn maatschappelijk functioneren wordt geraakt, betreft de toegang tot de overheid. Burgers moeten op redelijk gemakkelijke wijze toegang hebben tot essentiële informatie – bijvoorbeeld over wijze van aanvragen, geldende termijnen en kosten van reisdocumenten en vergunningen – en moeten in het algemeen kennis kunnen nemen van overheidsbeleid[1]. Op dit moment is Internet voor overheidsinformatie nog geen onontbeerlijk medium. De informatie die de overheid via diverse websites bekend maakt, is ook op andere wijze te verkrijgen. Burgers die geen toegang hebben tot de nieuwe communicatiemedia mogen echter niet op een achterstand worden gezet. Uitbreiding van de elektronische toegankelijkheid van overheidsinformatie vraagt derhalve ook om een actief toegangsbeleid.

3.2.2. Schaarsteproblemen

Een eerlijke verdeling van beschikbare radiofrequenties en van zendtijd zijn bij radio en TV belangrijke gronden voor overheidsinterventie. Internet is geen schaars medium. In tegendeel, Internet biedt iedereen de ruimte informatie beschikbaar te stellen. Bij de toegang tot de informatie via modem en Internet-serviceprovider kunnen zich echter wel degelijk schaarsteproblemen voordoen. Hierbij valt te denken aan het achterblijven van investeringen in de infrastructuur. Het gebruik van Internet neemt zo snel toe dat binnen enkele jaren capaciteitsproblemen zijn te verwachten. Een ordenende overheidsrol is derhalve niet uit te sluiten.

3.2.3. Vliegwieleffecten

Overheidsingrijpen wanneer de toegankelijkheid dat eist, is als middel om de ontwikkeling van Internet en e-mail te bevorderen zeer wel voorstelbaar. Daarmee geeft de overheid invulling aan haar faciliterende taak. Een algemene toegankelijkheid van Internet en goedkope e-mailfaciliteiten kunnen een belangrijke voorwaarde zijn voor het goed functioneren van de elektronische snelweg. Een aantal overheden heeft hiertoe al, soms ter uitvoering van het NAP, initiatieven ondernomen. Op deze manier tracht de overheid actief te bevorderen dat de elektronische snelweg zich tot meer ontwikkelt dan een middel voor amusement en hobbyisme. Tot nog toe is daarbij nog niet de inzet van een juridisch instrumentarium overwogen.

[1] Zie verder de Nota «Naar toegankelijkheid van overheidsinformatie», TK 20 644, nr. 30.

Het is de vraag of er redenen zijn het regime voor universele dienstverlening van de Telecommunicatiewet toe te passen op Internet en e-mail. Daarbij kan het gaan om de plicht voor een provider tot doorgifte van zijn dienst aan iedereen die daar om vraagt. En tegen redelijke kosten, ongeacht de plaats van vestiging. In eerste instantie wil de overheid dat aanbieders zelf komen tot universele dienstverlening. Maar waar de overheid de toegang van marktpartijen via concessieverlening controleert, kan universele dienstverlening worden afgedwongen.
Uitbreiden van het principe van universele dienstverlening tot Internet is op dit moment niet opportuun. Het is bij lange na niet bekend wat het toekomstige nut en gebruik van Internet wordt. Zelfs is, gezien de ontwikkeling naar Internet-II voor wetenschappers en het ontstaan van intranetten met gecontroleerde toegang, niet geheel duidelijk of Internet wel als eenheid blijft bestaan. Op dit moment is Internet vooral een raadpleeg- en communicatiemedium.
Mocht echter blijken dat een bepaalde maatschappelijk belangrijke functie, zoals het verrichten van betalingen, zich geheel naar Internet of een andere elektronische infrastructuur verplaatst, dan kan dat wel degelijk een reden zijn om het regime van de Telecommunicatiewet ook toe te passen op Internetdiensten en e-mailvoorzieningen. De reden daarvoor is overigens niet zozeer het vliegwieleffect, alswel het maatschappelijk functioneren van de burger.

3.2.4. Toegankelijkheid van wetenschappelijke informatie

Wetenschap kan alleen goed (objectief en betrouwbaar) functioneren bij een onbelemmerd verkeer van gegevens, ideeën, theorieën, informatie en documenten tussen onderzoekers. Beperkingen van dit informatieverkeer schaden de ontwikkeling van kennis van onze kennisafhankelijke samenleving. De toegenomen maatschappelijke betekenis van digitale informatie en kennis vertaalt zich in verdergaande wettelijke bescherming van bijvoorbeeld intellectuele eigendom en de persoonlijke levenssfeer. Daarmee worden drempels opgeworpen tegen de toegankelijkheid van wetenschappelijke informatie.
De Auteurswet kent bijvoorbeeld geen bescherming van feiten. De EU Richtlijn betreffende de rechtsbescherming van databanken[1] beschermt alleen de «extractie» van feiten uit een databank. Waar een steeds belangrijker volume aan wetenschappelijke gegevens zonder databanken de facto niet meer raadpleegbaar is, kunnen exclusieve rechten van databankproducenten het gebruik van deze gegevens bemoeilijken. En aan het gebruik van persoonsgegevens voor sociaal-wetenschappelijk onderzoek en medisch onderzoek worden steeds strengere eisen gesteld. Deze spanning vraagt aandacht van de wetgever voor de grotere algemene belangen die zijn gemoeid met wetenschappelijk onderzoek en van de wetenschapper meer oog voor het belang van adequate zelfregulering (in overeenkomsten en beroepscodes).

3.2.5. Toewijzing domeinnamen

Een ander vraagstuk is dat van de zogenaamde second-level domeinnamen. Deze domeinnamen vormen een elektronisch adres en zijn bepalend voor de adressering van e-mail verkeer en van www-sites. Voor de zogenaamde *generic top-level* domeinen (bijvoorbeeld *.com*) vindt toewijzing plaats door buitenlandse instellingen. Deze situatie wordt nu herzien, in het kader van het project *Generic Top-Level Domain Memorandum of Understanding,* in de Verenigde Staten op gang gebracht door de *Internet Society en de Assigned Numbers Authority.*
Voor het aan Nederland gerelateerde top-level domein «.nl» vindt toewijzing plaats door tussenkomst van de Stichting Internet Domeinregistratie Nederland, waarbij het gros van de actieve service-providers is

[1] PbEG 1996, L77.

aangesloten. Deze stichting heeft voor dit doel een toewijzingsreglement vastgesteld. Dit stelsel voorziet in een aantal publieke belangen. Men kan in dit verband bijvoorbeeld denken aan de transparantie van toewijzing, de eerbiediging van rechten van intellectuele eigendom en het vermijden dat bepaalde woorden gemonopoliseerd worden. Het kabinet zal er op toezien dat dit stelsel voldoet aan de eisen voor zelfregulering, zoals geformuleerd in Deel IV van de nota. Zonodig kan in aanvulling op dit stelsel publiekrechtelijke regelgeving worden voorbereid. Het kabinet zal hierover in overleg treden met de Stichting Internet Domeinregistratie Nederland.

4. Pluriformiteit en uitingsvormen

De overheid heeft de zorg op zich genomen om zowel de verspreiding als de kwaliteit van informatie in gunstige zin te beïnvloeden. Met het toegangsbeleid beoogt de overheid een goede bereikbaarheid van informatiekanalen te regelen. Met beleid gericht op pluriformiteit van informatie tracht de overheid de diversiteit en kwaliteit van informatie te verhogen. Ook hier is het uitgangspunt dat marktwerking alleen niet altijd voldoende is. Dit vraagstuk valt in enkele deelonderwerpen uiteen.

4.1. Mediabeleid

Burgers moeten toegang hebben tot verscheidene media en informatiebronnen, omdat ze kennis moeten kunnen nemen van informatie over het reilen en zeilen van de maatschappij, de overheidsorganen, de economie en de politiek. Toegang tot veelsoortige informatie over de maatschappij is van levensbelang voor onafhankelijke meningsvorming en daarmee voor het functioneren van de democratie. In het verleden is dit de aanleiding geweest voor pers- en omroepbeleid. De kern van het probleem is hier: wat is de toekomst van de media? Gaan kranten, opiniebladen en informatieve televisie-uitzendingen in de toekomst exclusief, of voor een zeer belangrijk deel gebruik maken van Internet en dan met name het multimediagedeelte: het World Wide Web? Of verdwijnen ze zelfs helemaal ten gunsten van nieuwe, interactieve media? Indien dat niet zo is, kunnen de huidige beleidskaders voor de pers volstaan. Waar echter die media, die voor de pluriformiteit van informatievoorziening cruciaal zijn, in meerderheid «achter het modem» verdwijnen, zal de overheid de toegankelijkheid van die informatie moeten garanderen.
Op dit moment speelt dit niet, omdat de traditionele media alleen gebruik maken van Internet om extra service te bieden, of als extra informatiekanaal. Alleen sommige wetenschappelijke publicaties, speciaal op de Internet-gemeenschap gerichte publicaties en bijzondere nieuwsbrieven, zijn uitsluitend via Internet bereikbaar. De beschikbare bandbreedte voor bijvoorbeeld uitgevers, is echter te beperkt voor optimaal gebruik van nieuwe technieken. Als de bandbreedte of de snelheid van datatransport, door de komst van een glasvezelnet, een ISDN-net of door grote versnelling van huidige technieken, toeneemt, kan het Internet een aanvaardbaar alternatief worden. Op dat moment is toegang tot het Internet noodzakelijk om toegang te krijgen tot pluriforme informatie. Het is overigens niet zo dat dan automatisch voor de overheid een rol ontstaat om die toegang te verzekeren. De genoemde technieken zullen voor content-providers namelijk pas interessant zijn als zich een voldoende grote markt heeft gevormd, ofwel, als een groot aantal mensen zich toegang heeft verschaft tot Internet. Marktwerking kan hier grote groepen burgers toegang garanderen. Dit laat echter onverlet dat er burgers zullen zijn voor wie toegang tot geavanceerde communicatiemiddelen niet gemakkelijk is. Hetzij omdat hen de financiële middelen ontbreken, hetzij omdat de kennis ontbreekt.

Internet en «on-line» diensten vallen niet onder de Mediawet. Ook in EU-verband is er nog geen regeling voor de nieuwe interactieve media. Deze vallen niet binnen het bereik van de richtlijn Televisie zonder grenzen. Het ontbreken van regulering met betrekking tot de nieuwe diensten kan aanleiding geven tot problemen waar nieuwe en traditionele media samenkomen. Een voorbeeld hiervan is het volgende: het is nu al mogelijk met speciale voorzieningen televisieprogrammas via de computer te ontvangen. Duitsland is er daarom toe over gegaan een kijk- en luisterbijdrage te gaan heffen op computers met een Internetaansluiting. De betalingsverplichting voor netsurfers in Duitsland is gebaseerd op het feit dat radio-uitzendingen steeds vaker rechtstreeks via Internet te beluisteren zijn.
Deze ontwikkeling doet zich ook in Nederland voor, maar in de huidige Mediawet vallen interactieve media niet onder het begrip «programma» en hoeft er ook geen kijk- en luisterbijdrage te worden betaald. Ook de regels uit de Mediawet met betrekking tot uitzendtijden van bepaalde programma's zijn, als die programmas via Internet beschikbaar zijn, loos geworden. Aanpassing van de Mediawet kan op termijn nodig zijn.
Niet alleen de Mediawet biedt echter regels over media, maar ook de nieuwe Telecommunicatiewet regelt onderwerpen op dit terrein, zoals de doorgifteplicht. Waar de media en de telecommunicatie naar elkaar toegroeien en het onderscheid tussen telecommunicatie en omroep niet goed meer te maken is, kan het problemen geven dat dergelijke onderwerpen onder verschillende wettelijke regimes vallen. Dit kan ook, wat betreft het toezicht, leiden tot afbakeningsproblemen tussen het Commissariaat voor de Media, de OPTA en de NMA.
Als de elektronische snelweg zich ontwikkelt tot een cruciaal medium voor de politieke en culturele pluriformiteit, valt te overwegen om het stimuleringsregime, zoals dat bestaat voor de traditionele media, bijvoorbeeld via het bedrijfsfonds voor de pers of publieke radio- en tv-produkties, ook toe te passen op de nieuwe media.

4.2. Politieke meningsvorming

Een democratische samenleving functioneert alleen goed als er voldoende «concurrentiemogelijkheden» in de politieke meningsvorming zijn. De diversiteit van meningen moet gewaarborgd zijn en niet alleen die meningen die commercieel aantrekkelijk zijn of geen schade toebrengen aan commerciële belangen moeten gehoord kunnen worden. Ook moet het niet zo zijn dat politieke macht toevalt aan hen die één of meer informatiemedia beheersen, althans niet louter op grond van die beheersing. Het is echter denkbaar dat een actor met voldoende zeggenschap over de inhoud en programmering van media die positie gebruikt om de publieke opinie te bespelen. De kernvraag is of er in een informatiesamenleving meer of minder mogelijkheden zijn om de media te beheersen en welke rol de overheid moet spelen bij het bewaken van een pluriform aanbod van politieke, of voor politieke meningsvorming belangrijke informatie. Het antwoord is niet eenduidig: er is op dit moment geen sprake van een eenvormige tendens.
Aan de ene kant is er ook in de media en op informatiemarkten een «normale» trend naar concentratie van kennis en kapitaal waar te nemen. Ook het eerder genoemde cross-owner-ship zal zich voordoen. In beginsel kunnen dergelijke concentraties met het mededingingsinstrumentarium worden aangepakt. Er zijn echter situaties denkbaar waarin een machtsconcentratie de mededingingstoets kan doorstaan, maar waarin een machtsconcentratie desalniettemin leidt tot een verschraling van het informatieaanbod. Er is in het verleden wel gepleit voor fusiecontrole op inhoudelijke gronden onder meer bij de dagbladpers, maar tot een wettelijke regeling is het nooit gekomen, hoewel in sommige sectoren zelfregulering plaatsvindt. Daarnaast spelen ook redactiestatuten bij

kranten en omroepen een belangrijke rol. Naarmate informatie een belangrijker rol gaat spelen in de samenleving, zal de vraag naar een goede wettelijke regeling van informatiemonopolies zich echter weer kunnen opdringen. Nader onderzoek is hiernaar dan ook geboden.
De verandering in de bezitsverhoudingen is een andere trend. Steeds meer bedrijven in de mediasector laten zich op de beurs noteren. Dat verspreidt het bezit van media- en informatiebedrijven over meer deelnemers: zowel individuele beleggers als institutionele beleggers. Dat kan in principe een diversiteit aan belangen en wensen genereren, die er voor zorgt dat ondernemingen niet simpelweg zijn te identificeren met één belang.
Naast de traditionele media komt ook Internet als medium van betekenis op. Wat Internet anders maakt dan andere media is het sterk decentrale karakter: er is geen centrale autoriteit die kan bepalen wat er op Internet verschijnt, het is zeer gemakkelijk informatie op Internet te plaatsen en het is niet gemakkelijk om gebruikers naar een bepaalde bron van informatie toe te leiden. De betekenis van Internet voor de politieke meningsvorming is moeilijk in te schatten, maar gezien de veelheid van politieke debatten op Internet kan het medium uitgroeien tot een belangrijk meningsvormend instrument. Internet is echter een fundamenteel onbeheersbaar medium. Internet kan gezien de sterk decentrale inslag dus tegenwicht bieden tegen de tendens tot centralisatie en concentratie van media.

4.3. Culturele uitingen

De komst van nieuwe media kan ook de culturele pluriformiteit verkleinen. Internet is een goed voorbeeld van een medium met culturele dominantie: de Amerikaanse taal en beeldcultuur zijn de «normale» uitingen op Internet. Mogelijk leidt dit tot een soort «Disney-effect», een hegemonie van Amerikaanse cultuuruitingen.
Er is echter ook een ander scenario mogelijk. Het zou kunnen dat de Amerikaanse dominantie een gevolg is van het feit dat Internet nog niet zo lang een massamedium is en dat de eerste echte groei in de VS heeft plaatsgevonden. In dat geval kan worden verwacht dat andere culturen wat meer tijd nodig hebben om een plaats op Internet te vinden. Uiteindelijk kan het Internet dan toch uitgroeien tot een verzamelplaats van verschillende culturen. Dat het Internet ruime mogelijkheden biedt aan weinig bekende en soms vreemde culturele uitingen is bekend; uitstervende talen kunnen via het Internet in leven blijven en het Klingon (een echte taal, gemaakt voor de populaire TV-serie Star Strek) is een voorbeeld van een taal die via de elektronische snelweg tot leven is gekomen en in leven wordt gehouden. Voor de inzet van een juridisch instrumentarium is geen aanleiding. Het internationale karakter van de elektronische snelweg moet als een gegeven worden beschouwd.

4.4. Schadelijke inhoud van uitingen

Het ontstaan van nieuwe informatiediensten leidt tot een ingrijpende wijziging van de context van de bescherming van minderjarigen. Deze bescherming is bij de regulering van de media altijd een factor van belang geweest. De opkomst van nieuwe media en een toename van het aanbod bij bestaande media, in een tijd dat de gezinsstructuur en het arbeidspatroon aan sterke veranderingen onderhevig zijn, leidt er toe dat kinderen meer dan vroeger in aanraking kunnen komen met schadelijk beeldmateriaal. Tegelijkertijd is er onder wetenschappelijke onderzoekers een groeiende consensus dat geweld in de media potentieel schadelijk is[1]. Krachtens de notitie «Bescherming van jeugdigen tegen schadelijke invloeden van audiovisuele media» wil Nederland jeugdigen een meer effectieve bescherming bieden. Ter verwezenlijking hiervan wordt er

[1] IIK 25 266, COM(96) 483 def.

gekozen voor zelfregulering, dit onder meer door de grondwettelijke beperkingen. Zie hiervoor verder Deel II C-4 van de nota.
Voor de televisie bestaan wettelijke beperkingen, voortvloeiend uit de Richtlijn TV zonder grenzen. Verder wettelijk ingrijpen – op Internet – wordt afgewezen, aangezien zon ingrijpen gauw te globaal is en de vrije meningsuiting in gevaar brengt.

5. Conclusies en voorstellen

5.1. Mededinging

- Hoewel informatie- en communicatiemarkten in beginsel aan dezelfde wetmatigheden onderhevig zijn als andere markten, vragen zij op korte termijn toch bijzondere aandacht. Er zal scherp moeten worden toegezien of het huidige mededingingsregime effectief is, gegeven het jonge, turbulente, internationale en vooral ook gelaagde karakter van informatiemarkten.
- Het thans ontwikkelde wetgevingskader – de Mededingingswet, Telecommunicatiewet en de Europese regelgeving – biedt voorlopig voldoende instrumenten voor het bevorderen van marktwerking op de nationale informatie- en communicatiemarkten.
- De hoge mate van technologische turbulentie en het jonge karakter van de markten vragen om een regelmatige monitoring van de ontwikkelingen en beoordeling van de effectiviteit van de activiteiten van de NMA en de OPTA. Het kabinet zal deze monitoring en beoordeling ter hand nemen en daarbij de conclusies en voorstellen van het MDW-rapport over het toezicht bij geprivatiseerde nutsvoorzieningen in acht nemen.
- Het kabinet zal stappen ondernemen om te komen tot nadere internationale afspraken die de samenwerking tussen mededingingsautoriteiten bevorderen. Deze stappen worden op EU-niveau ingezet.
- Standaardisatie van technische normen en koppelvlakken is een belangrijke voorwaarde voor het ontstaan van transparante informatie- en communicatiemarkten. Het kabinet hecht eraan dat er op dit vlak zelfregulering, bij voorkeur via internationale standaardisatieorganisaties, tot stand komt. De overheid zal de totstandkoming ervan actief bevorderen. Zelfregulering zal echter niet mogen leiden tot misbruik van dominante marktposities.
- Belangrijke standaards kunnen door dwanglicentiëring algemeen geldend worden gemaakt.
- Bij misbruik van Octrooirecht door een dominante partij kunnen mededingsregeling toepasselijk verklaard worden.
- Het kabinet zal onderzoeken of het zinvol is om het regime van de Telecommunicatiewet op het gebied van interconnectie ook toe te passen op andere informatiemarkten.

5.2. Toegankelijkheid

- Er is op dit moment nog geen aanleiding voor het inzetten van juridische instrumenten ter bevordering van de toegankelijkheid van de elektronische snelweg. Dit kan anders worden zodra de elektronische snelweg een niveau van ontwikkeling bereikt, waarin sprake is van verdringing. Bijzondere aandacht is nodig voor toegang tot de overheid.
- Toepassing op het Internet van het regime voor universele dienstverlening van de Telecommunicatiewet is op dit moment niet aan de orde. Dat kan veranderen indien Internet voor het instandhouden van maatschappelijke contacten een even belangrijk medium wordt als de telefoon., of deze zelfs vervangt. Het kabinet stelt voor om dit onderwerp over enkele jaren nogmaals te bekijken.

- Algemene toegangsvoorzieningen op het gebied van Internet zijn geboden indien overheden exclusief, of in zeer belangrijke mate informatie via Internet aanbieden, of de communicatie met overheidsfunctionarissen in belangrijke mate via Internet moet plaatsvinden.
- Een ordenende rol voor de overheid bij de toegankelijkheid tot de Internet-infrastructuur moet in de nabije toekomst niet worden uitgesloten. Het kabinet stelt voor dit onderwerp nader te bezien.
- Voor het aan Nederland gerelateerde top-level domein «.nl» vindt toewijzing plaats door tussenkomst van de Stichting Internet Domeinregistratie Nederland. Het kabinet zal er op toezien dat dit stelsel van zelfregulering voldoet aan de eisen voor zelfregulering, zoals geformuleerd in Deel IV van de nota. Zonodig kan in aanvulling op dit stelsel publiekrechtelijke regelgeving worden voorbereid. Het kabinet zal hierover in overleg treden met genoemde stichting.

5.3. Pluriformiteit

- De bepaling van de rol van de overheid bij het instandhouden van pluriformiteit op de elektronische snelweg is minder duidelijk. In een situatie waarin de elektronische snelweg pluriformiteit genereert, zoals dat op Internet gebeurt, is er geen specifieke rol voor de overheid weggelegd.
- Indien de elektronische snelweg zich ontwikkelt tot een cruciaal medium voor de politieke en culturele pluriformiteit, valt te overwegen om het stimuleringsregime dat thans bestaat voor de traditionele media ook daarop toe te passen. Natuurlijk zal de publieke omroep daarbij zijn rol spelen.
- Indien voor meningsvorming belangrijke media achter het modem verdwijnen, moet worden overwogen om deze media weer toegankelijk te maken door de toegang tot Internet te vergroten. Het kabinet stelt voor om dit onderwerp over enige jaren nogmaals te bezien.
- Convergentie van media en toenemende complexitiet van de informatiemarkt kunnen op termijn vragen om een hernieuwde afstemming van de wettelijke en toezichtregimes op het terrein van de media en de telecommunicatie. Deze afstemming wordt in ieder geval over enige jaren nader bezien.
- Naarmate informatie een belangrijker rol gaat spelen in de samenleving, wordt de behoefte aan een goede wettelijke regeling van informatiemonopolies groter. Van belang hierbij zijn de resultaten van het onderzoek naar cross-ownership in de mediasector.

F. RECHTSHANDHAVING

1. Inleiding

In Deel III B komt de handhaafbaarheid van wetgeving in de elektronische omgeving aan de orde in relatie tot de internationalisering. Dit hoofdstuk bekijkt de handhaving, het sluitstuk van wetgeving, in meer algemene zin.

Deze nota gaat uit van drie belangrijke kenmerken van de elektronische snelweg: dematerialisering, internationalisering en technologische turbulentie. Voor de handhaving speelt nog een vierde kenmerk een belangrijke rol, namelijk anonimiteit: het verhullen van persoonsgegevens op de elektronische snelweg en de onbekendheid van de persoon die de computer bedient.
Deze kenmerken kunnen de rechtshandhaving moeilijker maken. Aan de andere kant bieden de toegenomen technologische mogelijkheden de rechtshandhaving juist kansen, zoals het bevragen van gegevensbestanden.

Het hoofdstuk wordt onderverdeeld in een paragraaf over de strafrechtelijke handhaving en een paragraaf over privaatrechtelijke handhaving

2. Strafrechtelijke rechtshandhaving

2.1. Inleiding

De opkomst van het gebruik van moderne informatie- en communicatietechnologie brengt een eigen criminaliteitsbeeld met zich mee. Deel II C-3 beschrijft drie categorieën delicten, die op de elektronische snelweg een rol spelen: aantasting van het goed functioneren van informatiesystemen, vermogensdelicten en uitingsdelicten. Deze nieuwe vormen van criminaliteit vragen om een adequate strafrechtelijke aanpak. Immers, ook in de digitale omgeving mag de burger rekenen op een behoorlijk niveau van rechtshandhaving. Voor rechtshandhaving op de elektronische snelweg zijn enkele uitgangspunten van belang:

- Gedragingen, die «off-line» strafbaar zijn, zijn on-line evenzeer strafbaar. Om dit uitgangspunt te kunnen waarmaken, is ook een effectieve handhaving vereist.
- Er dient steeds – zowel bij het toekennen van handhavingsbevoegdheden als bij het toepassen daarvan – een zorgvuldige afweging te worden gemaakt tussen het belang van de rechtshandhaving en de inbreuk die wordt gemaakt op de privacy van de burger.
- De ontwikkeling van de elektronische snelweg wordt zoveel mogelijk aan de markt overgelaten. Dit betekent onder meer dat zo min mogelijk beperkingen worden opgelegd aan de toelating en het gebruik van technieken, zoals cryptografie.

Zelfregulering is in de afgelopen periode steeds een voornaam uitgangspunt geweest bij de handhaving van uitingsdelicten op de elektronische snelweg. Dit stelt eisen aan de strafrechtelijke handhaving, als publiekrechtelijke waarborg van de zelfregulering. Op het gebied van de bestrijding van kinderpornografie via Internet heeft de Minister van Justitie in een brief[1] aan de Tweede Kamer medegedeeld dat een actief opsporingsbeleid is geïndiceerd.

Deze uitgangspunten impliceren vooral dat de instanties die zijn belast met opsporing en vervolging, kunnen beschikken over toereikende strafvorderlijke bevoegdheden, die zijn toegesneden op de specifieke kenmerken van de elektronische snelweg. De belangrijkste opsporingsmiddelen worden beschreven in Deel II C-3. Recapitulerend:

[1] IIK 25 078, nr. 6.

- De Wet Computercriminaliteit heeft geleid tot de eerste specifiek op de elektronische snelweg toegesneden bevoegdheden.
- Het Wetsvoorstel Bijzondere opsporingsbevoegdheden omschrijft een aantal bevoegdheden dat ook geschikt is voor de elektronische snelweg.
- Het voorontwerp van de Wet Computercriminaliteit II vult enkele specifieke bevoegdheden aan in verband met nieuwe technologische ontwikkelingen.

Dit onderdeel van de nota richt zich vooral op de handhaving van misdrijven. Bij overtredingen speelt een ander probleem: het valt niet uit te sluiten dat in sommige gevallen handhaving niet meer mogelijk is. Immers, internationale rechtshulpverdragen hebben vaak geen betrekking op overtredingen. Als complicerende factor komt daar nog bij dat juist bij overtredingen de materiële normen nogal eens uiteenlopen. Daarnaast zullen ook niet alle technologische mogelijkheden kunnen worden ingezet bij de opsporing van overtredingen. De bescherming van de privacy verzet zich daartegen. Bij lichtere overtredingen wordt de inbreuk op de privacy dan niet gerechtvaardigd door het belang van de opsporing.

2.2. De effectiviteit van de handhaving: aftappen van telecommunicatie

Het aftappen is een veel gehanteerde bevoegdheid die aanzienlijk wordt beïnvloed door de ontwikkelingen op de elektronische snelweg, ten gevolge van technologie, maar ook van de door de EU ingezette liberalisering van de telecommunicatiemarkt. Telecommunicatie is vele decennia synoniem geweest voor openbare telefonie. Er was sprake van één dienst – spraaktelefonie – , van één aanbieder van de randapparatuur – PTT Telecom – en van één netwerkbeheerder – PTT Telecom. In de telecommunicatie voltrekt zich een aantal ingrijpende veranderingen.

- Er ontstaat een verscheidenheid van netten, apparatuur en diensten: draadgebonden, cellulaire en satellietnetten, telefonie-, fax-, video- en vele soorten datadiensten, maar ook apparatuur met uiteenlopende extra functies.
- Het aanknopingspunt voor een bevoegde tap is een verdachte of een aansluitnummer. Op last van de officier van justitie of de rechter-commissaris kan alle verdachte telecommunicatieverkeer worden afgetapt. Bij een grote verscheidenheid aan beschikbare telecommunicatiediensten, rijst de vraag hoe kan worden vastgesteld van welke telecommunicatienetten en -diensten de verdachte gebruik zal maken.
- Liberalisering van de telecommunicatiemarkt: veel marktpartijen en een scheiding van activiteiten van het aanbieden van diensten, van apparatuur en het exploiteren van een netwerk. Relevant voor het plaatsen van een bevoegde tap is het vinden van het aanspreekpunt: welke netwerkexploitant of service-provider moet de «tap» aanbrengen?
- Digitalisering van de telecommunicatie: er zijn veel verschillende codes voor digitalisering van spraak, afbeelding en video, er is data-compressie, er zijn computer-communicatieprotocollen en er zijn veel zeer krachtige versluierings- en versleuteltechnieken.
- Moderne telecommunicatiemiddelen zijn gebaseerd op digitale technieken. Twee partijen, die communiceren via digitale systemen, bedienen zich van dezelfde abstracte codes en fysieke signalen. Er is een enorme verscheidenheid aan abstracte codes voor de representatie van spraak, geluid, beeld en video beschikbaar.

Een tap gebeurt in principe in «real time» wanneer het gaat om personen op Nederlands territoir. Bij het tappen van berichtgeoriënteerde diensten, zoals e-mail, leidt dit tot de vraag of sprake is van transport of van opslag

van gegevens.[1] Er kan worden gesteld dat een gerechtelijk bevel tot tappen betrekking heeft op gegevens die worden getransporteerd, terwijl uitlevering of huiszoeking betrekking heeft op opgeslagen gegevens. Het achterhalen van bij een provider opgeslagen e-mail valt dus onder het regime van computerhuiszoeking. Een onderschepping tijdens het transport van het bericht (telecommunicatie) is tappen. Het tappen van e-mail kan plaatsvinden op de telefoonlijn waarmee de abonnee «inbelt» bij de Internet-provider, in het computersysteem van de provider, of op de verbindingen van de provider met de Internet-routers. Daarmee is medewerking van de provider vereist en daarin is thans wettelijk nog niet voorzien. Ingevolge de nieuwe Telecommunicatiewet wordt deze medewerking wel geregeld. Ook de ISP heeft, voor zover hij optreedt als telecommunicatiedienstaanbieder, de verplichting om tapvoorzieningen aan te brengen.
Uitgangspunt van de nieuwe Telecommunicatiewet is aftapbaarheid van openbare telecommunicatienetten en -diensten. Dit uitgangspunt zal ook voor de toekomst gehandhaafd blijven. Telecommunicatie vormt immers vaak de spil van criminele organisaties. Hiertoe zijn de volgende maatregelen nodig:

- In verband met technologische ontwikkelingen moet worden voorzien in een goed ingebed en gestructureerd overleg tussen politie en justitie enerzijds en vertegenwoordigers van telecommunicatie-aanbieders anderzijds.
- Er wordt een centraal informatiepunt ingericht voor het verkrijgen van abonneegegevens ten behoeve van het bevoegd aftappen.
- Er mag geen benadeling ontstaan van een exploitant of aanbieder van telecommunicatie ten opzichte van een concurrent. Voor zover de wettelijke eisen met betrekking tot tappen in de praktijk tot discriminatie leiden, kan een nadere invulling van die eisen noodzakelijk blijken.
- Onderzoek naar de vraag in welke vorm in het Wetboek van Strafvordering een bevoegdheid moet worden opgenomen die inhoudt dat derden verplicht kunnen worden om uit een door hen in stand gehouden persoonsregistratie een gegeven te verstrekken. Zie daarvoor Deel II C-3 van deze nota.

2.3. De effectiviteit van de handhaving: bijzondere opsporingsbevoegdheden

De bijzondere opsporingsbevoegdheden die van belang zijn in de elektronische omgeving zijn uitgebreid beschreven in Deel II C-3. Het gebruik van deze bevoegdheden kan een inbreuk opleveren op de soevereiniteit van een ander land. Een goed voorbeeld: infiltratie door de Nederlandse politie in een discussiegroep op Internet, waaraan een Nederlander deelneemt die er van wordt verdacht lid te zijn van een criminele organisatie. De vraag is dan aan welke overige voorwaarden moet zijn voldaan, zodat de Nederlandse politie ook daadwerkelijk in een discussiegroep kan infiltreren, ook op buitenlandse computers.
Er is hier sprake van een groot verschil met de traditionele toepassing van opsporingsbevoegdheden die inbreuk maken op de soevereiniteit van een ander land. Er is geen fysieke aanwezigheid nodig in het land waarvan de rechtsorde wordt geraakt. Immers, vanuit Nederland kan op de elektronische snelweg een opsporingsbevoegdheid worden uitgeoefend die inbreuk maakt op de soevereiniteit van een ander land. De huidige internationale rechtshulpverdragen zijn hier nog niet op ingesteld.
Voorts dient een oplossing te worden gezocht voor de in een elektronische omgeving noodzakelijke snelle reactie op rechtshulpverzoeken. De werkgroep «Crime in cyberspace» van de Raad van Europa ontwerpt een verdragstekst over internationale rechtshulp ten behoeve van het inwinnen van inlichtingen. In deze werkgroep is voorgesteld dat

[1] Zie voor het onderscheid tussen transport en opslag Deel II A van de nota.

opsporingshandelingen, die tevens gevolg hebben in een andere lidstaat, kunnen worden verricht, mits:
- deze – achteraf – worden genotificeerd en
- het land welks soevereiniteit door de maatregel is getroffen, achteraf voor het gebruik van de op deze wijze verkregen gegevens toestemming verleent.

Ook onderzoekt deze werkgroep de vragen omtrent rechtsmacht op de elektronische snelweg. Zoals uit Deel III B blijkt, is het immers niet altijd op voorhand duidelijk of bijvoorbeeld Nederland rechtsmacht heeft en, als dat zo is, welke landen daarnaast rechtsmacht kunnen claimen.
Het kabinet stelt voor om de werkzaamheden van de werkgroep van de Raad van Europa «Crime in cyberspace» uit te breiden. Deze groep zou zich ook moeten buigen over:
- het toepassen van bijzondere opsporingsbevoegdheden in de elektronische omgeving en
- de voorwaarden waaronder deze bijzondere opsporingsbevoegdheden in de elektronische omgeving mogen worden toegepast op het moment dat daardoor de soevereiniteit van een andere land wordt geraakt.

2.4. Het evenwicht met privacy

De strafvordering in de elektronische omgeving raakt op een groot aantal terreinen de privacy.
Zo is er een schat aan informatie over personen beschikbaar. Deze informatie is niet alleen te verkrijgen uit grote aantallen gegevensbestanden, maar ook uit de elektronische sporen die burgers op de elektronische snelweg achterlaten als bijvoorbeeld voor betalingen gebruik wordt gemaakt van een creditcard. Wanneer de overheid hierover de beschikking heeft, ligt in vergaande mate iemands levenswandel bloot. Door de toenemende risicos op inbreuken op de persoonlijke levenssfeer is een verdichting van de privacyregelgeving waarneembaar, waardoor afbreuk kan worden gedaan aan de rechtshandhavende capaciteit van de overheid. Teneinde een goed evenwicht te bereiken is het nodig de bevoegdheden die inbreuk maken op de privacy zo precies mogelijk te omschrijven. Voorts is nodig te zoeken naar handhavingsbevoegdheden die bij uitstek zijn toegespitst op handhaving in een informatiesamenleving. Zo zal nader onderzoek moeten plaatsvinden naar de noodzaak en de wenselijkheid van het gebruik van dataming als opsporingsmiddel. Bij dit onderzoek worden de volgende uitgangspunten gehanteerd:
- Opsporingsonderzoek naar en verwerken van gegevens is slechts toelaatbaar bij verdenking of bij een verkennend onderzoek, dan wel in verband met een onderzoek naar georganiseerde criminaliteit, zonder dat er sprake is van een concrete verdenking.
- Het verwerken van gegevens en de daarbij te gebruiken technieken kan een forse inbreuk op het recht op privacy opleveren. Een nauwkeurige afweging tussen het opsporingsbelang en het belang van de privacybescherming is nodig.

2.5. Privacy enhancing technologies (PET)

Deel III C van deze nota geeft aan dat ook op de elektronische snelweg anonimiteit uitgangspunt is. Die anonimiteit kan worden ondersteund met behulp van PET, technische middelen die de privacy op de elektronische snelweg kunnen beschermen, zoals de prepaid card voor mobiele telefonie.
Het opsporingsbelang kan een rechtvaardigingsgrond opleveren, om een inbreuk te maken op het recht op privacy. Zo heeft het kabinet recentelijk overwogen, dat bij aankoop van een prepaid card voor mobiele telefonie

identificatie vereist is. De aankoop zelf moet worden geregistreerd. Deze registratie wordt noodzakelijk geacht vanuit de gedachte dat juist criminelen van deze telefoonkaart gebruik maken, omdat die anonimiteit garandeert. Het is aannemelijk dat in de toekomst nog meer technische middelen worden aangeboden die het voor burgers mogelijk maken zich anoniem op de elektronische snelweg te begeven.
Het is de vraag of eisen als identificatie en registratie, die een inbreuk maken op het recht op privacy, voor alle PET moet worden gesteld. Tegenover de eisen die inbreuk maken op het recht op privacy zijn immers ook weer maatregelen nodig die een te grote inbreuk op het recht op privacy moeten voorkomen. Dit resulteert in een wettelijk stelsel dat steeds fijnmaziger wordt. Op deze wijze ontstaat er een soort regelgevingswedloop tussen enerzijds de bescherming van de privacy en anderzijds het opsporingsbelang. Met de komst van meer anonimiteit garanderende technische middelen, die door de individuele burger kunnen worden gebruikt, kan er daarom een moment komen waarop naar een nieuwe balans moet worden gezocht tussen het opsporingsbelang en het belang van de burger bij de bescherming van zijn privacy. Afhankelijk van de waardering van de in het geding zijnde belangen, zijn de volgende scenarios denkbaar:

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

Op termijn zal een keuze moeten worden gemaakt tussen beide scenario's. Een keuze waarbij te allen tijde identificatie en registratie is vereist, lijkt op voorhand niet aantrekkelijk.

2.6. De markt voorop

Bij de ontwikkeling van de informatiesamenleving is de markt leidend. De ontwikkeling van de infrastructuur wordt aan de private sector overgelaten. De ontwikkeling van diensten op die infrastructuur wordt aan zo min mogelijk belemmeringen onderworpen. Deze uitgangspunten hebben er onder meer toe geleid dat een verbod van cryptografieprodukten niet aan de orde is. Verder stelt de overheid geen technische eisen aan de infrastructuur, behoudens de medewerkingsverplichting van aanbieders van telecommunicatiediensten in de nieuwe Telecommunicatiewet.
Het behoeft geen betoog dat deze uitgangspunten de rechtshandhaving door de overheid bemoeilijken. Immers, technologische turbulentie op de markt eist ook van de overheid dat zij haar technologie en technologische kennis steeds aanpast. Bovendien kan het op de markt komen van voor de handhaving onwenselijke technologie niet worden voorkomen. Daarbij kan worden gedacht aan sterke cryptografie, maar ook bijvoorbeeld aan mobiele communicatie via satellieten en aan de prepaid card. Niettemin kunnen ook Trusted Third Parties een bijdrage leveren aan deze problematiek. Het wordt dan ook overwogen om in een juridisch kader voor TTP's de eis op te nemen dat TTP's voor zover zij niet uit andere hoofde daartoe zijn verplicht, in het kader van de opsporing en vervolging medewerking dienen te verlenen aan bevoegd gegeven bevelen.

2.7. Zelfregulering

Bij het bestrijden van kinderporno op Internet heeft zelfregulering van de providers een belangrijke rol gespeeld. Zozeer zelfs, dat deze vorm van zelfregulering thans bij de bestrijding van schadelijke en illegale inhoud het voorbeeld is voor de Europese Unie. Deel II C-3 van deze nota stelt voor het meldpunt uit te breiden tot andere delicten en andere categorieën tussenpersonen. Dit betekent niet dat zelfregulering de overheid ontslaat van haar taken op het gebied van de strafrechtelijke handhaving. De belangen die met het strafbaar stellen van handelingen zijn gediend, moeten immers primair door de overheid worden gewaarborgd.

2.8. Tot slot

Naast een toereikend wettelijke instrumentarium vormen een adequate organisatie, goed opgeleide politie- en justitiefunctionarissen en de beschikbaarheid van een kwalitatief hoogwaardige informatietechnologische uitrusting noodzakelijke voorwaarden voor een goede strafrechtelijke rechtshandhaving op de elektronische snelweg. De opbouw van de huidige organisatie van rechtshandhaving lijkt nog onvoldoende te zijn toegesneden om het hoofd te kunnen bieden aan de nieuwe vormen van criminaliteit.
Daarnaast lijken er binnen grote delen van politie en justitie kennishiaten te bestaan over een adequate rechtshandhaving op de elektronische snelweg. Dit kan relatief eenvoudig worden verholpen door extra investeringen in onderwijs. Ook de staande en zittende magistratuur zal op dit onderdeel bijscholing moeten worden aangeboden.
Over de voornemens op het gebied van organisatie, opleiding en uitrusting van politie- en justitiefunctionarissen met het oog op een goede strafrechtelijke rechtshandhaving op de elektronische snelweg zal de Tweede Kamer, na overleg met alle betrokkenen, voor het zomerreces van 1998 nader worden geïnformeerd.
Aan het openbaar ministerie zal worden gevraagd een officier van justitie aan te stellen die de landelijke coördinatie zal verzorgen van de opsporing op de elektronische snelweg. Mede vanwege het veelal ontbreken van een aanwijsbare plaats van het delict, is het nodig op landelijk niveau een aanspreekpunt te hebben. Tot slot is het van groot belang dat ruime ervaring wordt opgedaan met de toepassing van bijzondere opsporingsbevoegdheden op de elektronische snelweg.
De Minister van Justitie zal voorts het initiatief nemen voor een grootschalig onderzoek naar de aard, ernst en omvang van ICT-criminaliteit en het gebruik van bevoegdheden in dit verband. Resultaten daarvan kunnen eveneens in internationaal verband gebruikt worden. Ook kan dit onderzoek aanleiding geven tot de formulering van nieuwe delictsomschrijvingen voor het geval het gebruik van bestaande strafbaarstellingen in digitale omgeving problemen oplevert.

3. Privaatrechtelijke rechtshandhaving

3.1. Inleiding

Ook ten aanzien van burgerlijke rechten rijst de vraag of en, zo ja, hoe deze in de praktijk van de elektronische snelweg kunnen worden gehandhaafd. Hiertoe moeten in het bijzonder de bepalingen van het Wetboek van Burgerlijke Rechtsvordering worden bezien. Uitgangspunt is ook hier: de handhaving van burgerlijke rechten moet op de elektronische snelweg op hetzelfde niveau staan als in de traditionele omgeving. Immers, alleen dan zal de elektronische snelweg voor de burger een bruikbaar, want voldoende betrouwbaar, alternatief vormen. Overigens is het goed op te merken dat anders dan in het strafrecht, de overheid hier

slechts een beperkte rol speelt. Het is immers niet de overheid die handhaaft, maar de burger zelf. De overheid schept slechts randvoorwaarden en creëert waarborgen om de handhaving door de burger mogelijk te maken.

De handhaving van burgerlijke rechten op de elektronische snelweg kent drie fasen:
- De bewijsgaring (zie 3.2).
- Het in rechte geldend maken van burgerlijke rechten, inclusief de bewijslevering (zie 3.3).
- De tenuitvoerlegging van een rechterlijke of arbitrale uitspraak. Deze fase leidt niet tot bijzondere vragen en blijft hier verder buiten beschouwing.

De rol van het privaatrechtelijk beslag in de informatiesamenleving zal apart worden behandeld (zie 3.4).

3.2. Bewijsgaring

Dematerialisering brengt met zich mee dat in de toekomst steeds meer informatie in elektronische vorm beschikbaar zal zijn die kan dienen als bewijs in privaatrechtelijke kwesties. De toegankelijkheid van elektronische informatie en de mogelijkheid om vast te stellen of deze informatie wellicht ergens aanwezig is, zullen in de toekomst steeds belangrijker worden. In de praktijk zal de mate van toegankelijkheid steeds bepalen of het vergaren van voldoende bewijs mogelijk is of niet. En daarmee tevens de grens aangeven tussen een geslaagde vordering in rechte en een mislukte. Nu geldt iets soortgelijks uiteraard in een fysieke omgeving – ook daar moet men immers de hand weten te leggen op de goede stukken, of althans weten dat ze bestaan – maar de vluchtigheid en ongrijpbaarheid van elektronische informatie geeft aan dit probleem een extra dimensie, die nog wordt versterkt door de snelheid van de technologische ontwikkelingen. De informatiesamenleving brengt verder met zich mee dat informatievergaring ook internationaal gemakkelijker en sneller kan geschieden. Dit veronderstelt evenwel dat ook de burger ook toegang heeft tot de voordelen van de informatiesamenleving.

De vormvoorschriften uit het materiële privaatrecht, zijn niet zelden ingegeven door de gedachte dat moet worden verzekerd dat de partijen op een gegeven moment ook daadwerkelijk bewijs kunnen leveren. Deel II C-1 van deze nota wijst op de wenselijkheid van een juridisch kader voor TTP's. Het sluitstuk van zo'n juridisch kader zou moeten zijn: het verlenen van bewijskracht aan door TTP's vastgelegde elektronische informatie. Daarnaast wordt gedacht aan het totstandbrengen van een regeling inzake de digitale handtekening. In verschillende internationale fora houdt men zich bezig met de ontwikkeling van een dergelijke infrastructuur. Zo bereidt de Europese Commissie momenteel maatregelen voor inzake de digitale handtekening voor, waarbij wordt gedacht aan:
- minimumvereisten voor certificatie-autoriteiten,
- minimumvereisten voor certificaten,
- regels inzake gelijke behandeling van digitale en gewone handtekening in het bewijsrecht en
- het steunen van verdergaande mondiale samenwerking binnen organisaties als de OECD, de WTO en de Verenigde Naties.

Nederland zal op nationaal niveau op deze punten initiatieven ontwikkelen, uiteraard afhankelijk van de voortgang op EU-niveau. Afhankelijk daarvan zal nationale regelgeving worden voorbereid. Dit kan verschillende voordelen hebben. In de eerste plaats zou zulke regelgeving een voor Nederland positieve signaalfunctie hebben. Voorts kan op basis van nationale regelgeving expertise worden opgebouwd. Tenslotte zullen deze

ervaring en expertise ons land van nut zijn bij de inbreng in het internationale overleg.

3.3. Het in rechte geldend maken van burgerlijke rechten

3.3.1. Lijdelijkheid van de rechter; stelplicht en bewijslast

Voor het handhaven van rechten voor de burgerlijke rechter zijn de regels van stelplicht, bewijslastverdeling en bewijs van het grootste belang. In het burgerlijk procesrecht is de rechter immers lijdelijk, niettegenstaande de plicht tot het ambtshalve aanvullen van gronden. Hij mag slechts die feiten en rechten aan zijn beslissing ten grondslag leggen die in het geding te zijner kennis zijn gekomen en zijn komen vast te staan.

In een privaatrechtelijk geding is de bewijslast verdeeld over beide partijen. Hoofdregel daarbij is dat de bewijslast van bepaalde feiten of rechten rust op de eisende partij, tenzij uit een bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere verdeling voortvloeit. Het is uiteindelijk altijd de rechter die de bewijslast verdeelt. Hoewel de bewijsvoering in een elektronische omgeving wellicht tot andere vragen aanleiding zal geven dan in een traditionele, leidt het recht op het punt van de stelplicht en bewijslast niet tot problemen die specifiek zijn voor het gebruik van moderne technologie. Bovendien kan de rechter volgens het wettelijk systeem met alle omstandigheden rekening houden, dus ook met een elektronische context.

3.3.2. Het materiële bewijsrecht

Dematerialisering kan het leveren van bewijs gecompliceerder maken. Het is vervolgens een vraag van materieel bewijsrecht of het bewijs met behulp van de vergaarde elektronische – eventueel in combinatie met «tastbare» – bewijsmiddelen kan worden geleverd.

In de rechtspraak is tot dusverre nog vrijwel geen ervaring opgedaan met de waardering van elektronische bewijsmiddelen. Evenwel, het Nederlands bewijsrecht kent twee belangrijke uitgangspunten:

- Er bestaat een zogenoemd open systeem van bewijsmiddelen. Dat wil zeggen dat bewijs kan worden geleverd door alle middelen, tenzij de wet anders bepaalt. Elektronische bewijsmiddelen zijn dus toegelaten.
- De waardering van het bewijs is aan de rechter overgelaten, tenzij de wet anders bepaalt.

Deze twee uitgangspunten maken dat de rechter op het punt van de bewijsvoering een bijzonder grote vrijheid heeft. Deze vrijheid geeft hem de ruimte in te spelen op de ontwikkelingen inzake het elektronisch rechtsverkeer.

In wezen is hiermee de problematiek grotendeels teruggebracht tot een technische aangelegenheid. Indien partijen ervoor zorgen dat zij op het technische vlak de zaken deugdelijk hebben geregeld, mag ervan worden uitgegaan dat de rechter daaraan op het punt van de bewijslevering consequenties zal verbinden. Anders gezegd: zoals er gemakkelijk en minder gemakkelijk te vervalsen papieren documenten zijn en betrouwbare en minder betrouwbare getuigen, zo zullen er in een elektronische omgeving ook betrouwbare apparaten, technieken en methodieken bestaan. De technologische turbulentie speelt hier een belangrijke rol. De snelheid van de ontwikkelingen maakt het lastig om te bepalen of een bepaalde techniek op een gegeven moment nog voldoende betrouwbaar is.

Ook op dit punt kunnen regels over TTP's en de digitale handtekening voor partijen een belangrijke ondersteuning vormen. De overheid kan daarmee bewerkstelligen dat burgers met een grote mate van zekerheid kunnen voorspellen welke wijze van vastlegging van elektronische informatie met zodanige waarborgen is omkleed, dat de rechter daaraan voor het bewijsrecht gevolgen zal verbinden. Indien de mate van zekerheid die aan deze elektronisch vastgelegde informatie kan worden ontleend dat rechtvaardigt, kan de wetgever bepalen dat digitaal vastgelegde informatie in bepaalde gevallen een met informatiedragers uit de traditionele omgeving vergelijkbare bewijskracht heeft.

3.3.3. Bewijsovereenkomsten

Tot slot verdient hier de mogelijkheid van het sluiten van een bewijsovereenkomst vermelding. In een open omgeving, zoals Internet, is het lastig met bewijsovereenkomsten te werken. Daartoe heeft immers in beginsel iedereen toegang, zodat het niet goed mogelijk is ervoor te zorgen dat alle daarop opererende partijen zich aan bepaalde bewijsregels onderwerpen vóórdat zij met elkaar in contact komen (zie hiervoor verder Deel III C-1).

3.3.4. Alternatieve geschillenbeslechting

Handhaving van burgerlijke rechten is ook buiten de rechter om mogelijk. Te denken valt aan:
- arbitrage,
- bindend advies en
- conflictbemiddeling.

Arbitrage kent een eigen wettelijke, op internationale afspraken gebaseerde regeling in het Wetboek van Burgerlijke Rechtsvordering. Arbitrage komt veel voor bij handelsgeschillen, of in gevallen waarin een grote deskundigheid van de conflictbeslechter wordt verlangd. Er bestaat geen enkel formeel beletsel voor het toepassen van arbitrage op geschillen tussen partijen op de elektronische snelweg. De uitspraak van een arbitraal college heeft een werking die – na verlof van de president van de rechtbank – gelijk staat met een rechterlijke uitspraak.
Bindend advies komt in Nederland veel voor bij consumententransacties, waarbij geschillencommissies een rol spelen. Partijen verbinden zich contractueel het oordeel van de bindend adviseur te volgen.
Niet-nakoming van het bindend advies door de één, vormt wanprestatie tegenover de ander.
Op dit moment staan alternatieve wijzen van conflictbeslechting – dat is: zonder bemoeienis van de rechter – sterk in de aandacht, waarvan conflictbemiddeling een specifieke vorm is. Conflictbemiddeling kan ook de vorm krijgen van voorbereiding op een geschil voor de rechter, waarbij partijen hun conflict zodanig uitbenen dat de rechter mogelijk slechts de functie heeft van bekrachtiger van het bemiddelingsaccoord.

Het is denkbaar dat deze vormen van alternatieve geschillenbeslechting in de elektronische omgeving een voorname rol zullen spelen. Deze vormen bieden de mogelijkheid van een op maat gesneden uitspraak, of een regeling die tot stand komt na een op maat gesneden procedure.

3.4. Privaatrechtelijk beslag en andere maatregelen tot bewaring of tenuitvoerlegging van rechten

Het leggen van beslag is vooral van belang voor:
- Het voorkómen van (verdere) schade, het zekerstellen of boven water

krijgen van bewijs en het zekerstellen van een verhaalsobject in afwachting van het verkrijgen van een executoriale titel.
- Het inleiden van de executie van een goed waaromtrent reeds een executoriale titel (doorgaans een rechterlijke uitspraak) is verkregen.

Het beslag – in de praktijk wellicht het belangrijkste middel tot bewaring van recht – leidt vooral tot vragen in verband met dematerialisering in de informatiesamenleving. Het feit dat op de elektronische snelweg veel wat van economische waarde is, slechts in digitale vorm aanwezig is, betekent dat het privaatrechtelijk beslag in het kader van de handhaving een belangrijk deel van zijn nuttige functie zal verliezen indien het niet kan rusten op de gegevens zelf. In dat geval immers, zal slechts beslag kunnen worden gelegd op de stoffelijke drager van die informatie, zoals een diskette, een harde schijf en dergelijke. Voor een aantal gevallen zal dit een afdoende oplossing zijn, maar niet voor alle. De vraag wat een computerbestand nu eigenlijk in vermogensrechtelijke zin is en of daarop beslag kan worden gelegd, is dus van belang.

De wettelijke mogelijkheden tot beslag zijn beperkt tot bepaalde categorieën van goederen, niet exclusief stoffelijke objecten. Een wettelijke regeling die het beslag op elektronische opgeslagen gegevens met zoveel woorden mogelijk maakt, is er niet. Dit maakt dergelijke beslaglegging afhankelijk van rechterlijke interpretatie.
Voor bepaalde gevallen is deze problematiek reeds eerder onder ogen gezien en ook opgelost. Zo kent de Auteurswet een bijzondere regeling voor de «fysieke» vorm waarin het recht zich manifesteert. Deze vorm – de drager waarop of waarin het beschermd werk is belichaamd – is vatbaar voor beslag. De rechter verleent in de praktijk evenwel verlof tot het leggen van beslag op computerprogrammatuur, die is, of kan worden opgeslagen op een drager, tegelijkertijd met een bevel tot inbewaringgeving van deze diskette, of tot beveiliging van het betreffende bestand, of het betreffende programma voor de duur van de inbewaringgeving. Deze ervaringen kunnen als voorbeeld dienen voor hoe de rechter en de praktijk de bestaande bepalingen interpreteren en toepassen.

Het is duidelijk dat in bepaalde gevallen nogal wat haken en ogen kunnen zitten aan het beslag op de elektronische snelweg. Er zijn echter alternatieve, wettelijk geregelde instrumenten waarmee hierin – in ieder geval voor een belangrijk deel – kan worden voorzien. De rechter kan bijvoorbeeld – in de praktijk zal dat doorgaans in kort geding zijn – een verbod of bevel uitspreken. Zo kan iemand een rechterlijk bevel krijgen tot het verwijderen of tijdelijk ontoegankelijk maken van bepaalde gegevensbestanden. Een dergelijk verbod of bevel kan eventueel worden versterkt met een dwangsom. Voorts zijn met het nieuwe Burgerlijk Wetboek de mogelijkheden van zogeheten reële executie belangrijk uitgebreid. De wet stelt tegenwoordig voorop dat hij, die jegens een ander verplicht is iets te geven, te doen, of na te laten, daartoe op vordering van de gerechtigde in beginsel door de rechter wordt veroordeeld.
Het begrip reële executie wordt door de wet niet gedefinieerd. Het betekent in de praktijk vooral dat de schuldeiser die wordt geconfronteerd met een onwillige schuldenaar, in minder gevallen genoegen hoeft te nemen met schadevergoeding. Ook zal hij vaker in staat zijn datgene te verkrijgen waaraan de schuldenaar zich in eerste instantie had gebonden, of waarop hij anderszins recht heeft. Uiteraard zal met deze instrumenten ervaring moeten worden opgedaan op de elektronische snelweg. Maar in onderling verband bezien, lijken zij wel ruimte te bieden voor bevredigende oplossingen.

Indien deze bestaande alternatieve handhavingsinstrumenten in de praktijk niet bevredigend zouden blijken te werken, moet het worden

overwogen om een algemene regeling betreffende middelen tot bewaring van rechten in een elektronische omgeving – in het bijzonder beslag op gegevensbestanden – op te nemen in het Wetboek van Burgerlijke Rechtsvordering. Daarin zouden dan ook privacy- en andere maatschappelijke aspecten moeten worden opgenomen. Zo lijkt het logisch op e-mail beslag onmogelijk te maken, zoals ook artikel 11 van de Postwet beslag op de aan de post toevertrouwde postzendingen uitsluit.

4. Conclusies en voorstellen

4.1. Algemeen

- De rechtshandhaving on-line dient gelijke waarborgen te bieden als de rechtshandhaving off-line.
- Dematerialisering, internationalisering, technologische turbulentie en anonimiteit maken de rechtshandhaving moeilijker. Aan de andere kant bieden de technologische ontwikkelingen de rechtshandhaving juist kansen, zoals het nagaan van sporen op de elektronische snelweg.

4.2. Strafrechtelijke rechtshandhaving

- Bij het toekennen van strafrechtelijke handhavingsbevoegdheden dienen de volgende uitgangspunten te worden gehanteerd:
  - De elektronische snelweg mag geen rechtsvrij gebied worden.
  - De inbreuk die de handhaving maakt op de privacy van de burger moet steeds worden afgewogen.
  - Aan de ontwikkeling van de markt moet zo min mogelijk beperkingen worden opgelegd.
  - De kosten voor de gebruiker van de elektronische snelweg mogen niet onevenredig hoog zijn.
- De instanties die zijn belast met opsporing en vervolging dienen te kunnen beschikken over toereikende strafvorderlijke bevoegdheden, die zijn toegesneden op de specifieke kenmerken van de elektronische snelweg.
- Tappen dient ook in de toekomst mogelijk te blijven. Hiertoe is nodig:
  - Een goed ingebed en gestructureerd overleg tussen politie en justitie enerzijds en vertegenwoordigers van telecommunicatieaanbieders anderzijds.
  - Een centraal informatiepunt voor het verkrijgen van abonneegegevens ten behoeve van het bevoegd aftappen.
  - Er mag geen benadeling ontstaan van een exploitant of aanbieder van telecommunicatie ten opzichte van een concurrent. Voor zover de wettelijke eisen met betrekking tot tappen in de praktijk tot discriminatie leiden, kan een nadere invulling van die eisen noodzakelijk blijken.
  - Onderzoek naar de vraag in welke vorm in het Wetboek van Strafvordering een bevoegdheid moet worden opgenomen die inhoudt dat derden verplicht kunnen worden om uit een door hen in stand gehouden persoonsregistratie een gegeven te verstrekken. Zie daarvoor Deel II C-3 van deze nota.
- Ingevolge de nieuwe Telecommunicatiewet heeft ook de ISP, voor zover deze optreedt als aanbieder van telecommunicatiediensten, de verplichting om tapvoorzieningen aan te brengen en mee te werken aan een bevoegd gegeven bevel tot aftappen.
- In het kader van de Raad van Europa moeten afspraken worden gemaakt over specifieke rechtsmachtvraagstukken met betrekking tot de toepassing van opsporingsbevoegdheden op Internet.
- Er vindt onderzoek plaats naar het gebruik van datamining als

opsporingsmiddel. Daarbij worden de volgende uitgangspunten gehanteerd:
  - Het onderzoek naar en het verwerken van gegevens is slechts toelaatbaar bij een verdenking of een verkennend onderzoek, danwel in verband met een onderzoek naar georganiseerde criminaliteit zonder dat er sprake is van een concrete verdenking.
  - Het verwerken van gegevens en de daarbij te gebruiken technieken kunnen een forse inbreuk op het recht op privacy opleveren. De afweging tussen het opsporingsbelang en het belang van de privacybescherming dient daarom nauwkeurig plaats te vinden. Zo dient bijvoorbeeld in de wet duidelijk te worden gemaakt of het gaat om incidentele bevragingen op persoon, of dat ook datamining en soortgelijke technieken mogelijk is.
- Het wordt overwogen om in een juridisch kader voor TTP's de eis op te nemen, dat TTP's, voor zover zij niet uit anderen hoofde daartoe zijn verplicht, medewerking moeten verlenen aan bevoegd gegeven bevelen.
- Voor de zomer van 1998 zal de Tweede Kamer nader worden geïnformeerd over de voornemens op het gebied van organisatie, opleiding en uitrusting van politie- en justitiefunctionarissen, met het oog op een goede strafrechtelijke rechtshandhaving op de elektronische snelweg.
- De Minister van Justitie zal het initiatief nemen tot een onderzoek naar de aard, ernst en omvang van ICT-criminaliteit en het gebruik van bevoegdheden in dit verband.

4.3. Privaatrechtelijke rechtshandhaving

- Het wordt voorgesteld in het Wetboek van Burgerlijke Rechtsvordering een regeling op te nemen die voorziet in het verlenen van bewijskracht aan door bepaalde TTP's vastgelegde elektronische informatie.
- Het wordt voorgesteld om een regeling inzake de digitale handtekening tot stand te brengen, waarbij wordt aangesloten bij een binnenkort te verwachten voorstel voor EU-regelgeving.
- De bewijsovereenkomst kan voor zogenoemde gesloten netwerken van groot praktisch belang zijn.
- Alternatieve geschillenbeslechting, zoals arbitrage, bindend advies en conflictbemiddeling, kunnen in de elektronische omgeving een voorname rol spelen.
- Voor «beslag» op de elektronische snelweg wordt de rechtsontwikkeling vooralsnog aan de rechter over gelaten. Hij heeft daarvoor als instrumenten:
  - De rechter kan een verbod of bevel uitspreken. Zo kan iemand bijvoorbeeld een rechterlijk bevel krijgen tot het verwijderen of tijdelijk ontoegankelijk maken van bepaalde gegevensbestanden.
  - Reële executie.
- Het kabinet stelt voor om, zodra blijkt dat deze instrumenten in de praktijk niet bevredigend werken, een algemene regeling betreffende middelen tot bewaring van rechten in een elektronische omgeving – in het bijzonder beslag op gegevensbestanden – in het Wetboek van Burgerlijke Rechtsvordering op te nemen.

G. SAMENVATTING EN CONCLUSIES

In dit deel van de nota zijn vijf themas behandeld die van strategisch belang zijn bij de verdere ontwikkeling van de elektronische snelweg.

De thema's privacy, betrouwbaarheid en markten zijn in eerste instantie vooral van belang voor de gebruikers van de elektronische snelweg. Enkele belangrijke conclusies zijn:

- Deelname aan het elektronisch verkeer is in beginsel een verantwoordelijkheid van aanbieders en gebruikers zelf. Vraagstukken van betrouwbaarheid, toegankelijkheid en pluriformiteit zijn daarom in eerste instantie kwesties van vraag en aanbod.
- Gegeven het jonge en turbulente karakter van de ICT-markten, zal de nadruk in het overheidsbeleid voorlopig dienen te liggen op het stimuleren van marktwerking en zelfregulering door de betrokken maatschappelijke partijen.
- Op korte termijn is er voor de overheid vooral een faciliterende rol weggelegd. Zij dient er scherp op toe te zien dat de ICT-markten voldoende transparant en concurrerend zijn. Zij dient er voor te zorgen dat burgers voldoende in staat zijn om hun risico's en niveau van (privacy)bescherming te bepalen en zij dient het juridisch kader te verschaffen voor een ongestoord maatschappelijk verkeer. Ook dient zij de zelfregulering te stimuleren en waar nodig te ondersteunen.
- De overheid wordt daarbij geconfronteerd met twee maatschappelijke behoeftes die op gespannen voet met elkaar staan. Enerzijds is er een grote maatschappelijke behoefte aan flexibiliteit, omdat de ontwikkelingen complex en onvoorspelbaar zijn. Anderzijds vragen sommige ontwikkelingen ook om heldere en zekere kaders, ter bescherming van een aantal fundamentele waarden en normen van de democratische rechtsstaat. Dat laatste speelt vooral rond het thema privacy. Ook sommige aspecten van de juridische betrouwbaarheid vragen om meer zekerheden. Op het terrein van marktwerking kan met een meer terughoudende rol van de regelgever worden volstaan.
- Er is op deze drie terreinen op dit moment geen aanleiding voor breed opgezette vormen van overheidsregelgeving. De wetgevingskaders in de sfeer van telecommunicatie, bescherming van persoonsgegevens, burgerlijk recht en mededinging zijn onlangs aangepast of zullen binnenkort worden vernieuwd. Deze kaders zijn over het algemeen redelijk goed toepasbaar op het elektronisch verkeer.
- Wel is een reeks van aanpassingen nodig om er voor te zorgen dat off-line en on-line de juridische normen en instituties hetzelfde zijn en dat nieuwe ontwikkelingen zoals biometrie, TTP's en PET, worden gefaciliteerd. De nota bevat hiertoe een aantal voorstellen.
- Gegeven het internationale karakter van veel elektronisch verkeer en van de ICT-markten zijn internationale afspraken veelal onontbeerlijk.

Deze betrekkelijk beperkte taakstelling voor de overheid vloeit ten dele voort uit de constatering dat de elektronische snelweg vooralsnog een aanvulling vormt op het traditionele, analoge maatschappelijke verkeer. Burgers en bedrijven blijven voorlopig de mogelijkheid houden om zich van de klassieke media en communicatiemiddelen te bedienen. Wie zich op de elektronische snelweg begeeft doet dit in beginsel uit vrije wil en op eigen risico.

Op wat langere termijn is echter voorstelbaar dat de elektronische communicatie op sommige terreinen de traditionele communicatie verdringt. Burgers en bedrijven die zich niet van de elektronische snelweg (kunnen) bedienen worden dan ernstig in hun maatschappelijk functioneren gestoord. Een dergelijke ontwikkeling heeft belangrijke gevolgen voor de overheidsrol:

- Indien het belang van elektronische communicatie zo groot wordt dat

burgers en bedrijven daarzonder maatschappelijk niet meer goed kunnen functioneren, zal de overheid een meer actieve rol dienen te spelen.
- Deze actievere rol zou zich bijvoorbeeld kunnen uiten in een verscherpt toezicht op een betrouwbare en ongestoorde elektronische communicatie, een specifiek toegankelijkheidsbeleid voor (onderdelen van) de elektronische snelweg, een stimuleringsbeleid voor politieke en culturele uitingen en de vervanging van zelfregulering door wettelijke regimes, bijvoorbeeld op het terrein van de privacy.
- Overheidsondersteuning en -regelgeving is in ieder geval geboden wanneer de overheid zelf van burgers eist dat zij met haar langs elektronische weg communiceren of wanneer de overheid in overwegende mate haar informatie en diensten langs elektronische weg aanbiedt.

De thema's internationalisering en rechtsmacht en rechtshandhaving zijn vooral van strategisch belang voor de overheid zelf. Zij betreffen haar rol van hoeder van de rechtsstaat op de elektronische snelweg. Enkele belangrijke conclusies op deze terreinen zijn:
- Een van de kerntaken van de overheid op de elektronische snelweg is het waarborgen van de fundamentele normen en waarden van de democratische rechtsstaat.
- Specifieke kenmerken van de elektronische snelweg, zoals dematerialisering, internationalisering, technologische turbulentie en anonimiteit, stellen de rechtshandhaving voor grote problemen. Met name de internationalisering maakt het voor nationale overheden soms zeer lastig om het nationale recht te handhaven. Dit speelt in het bijzonder in de sfeer van het strafrecht.
- De noodzaak van een adequate strafrechtelijke opsporing van delicten op, of met behulp van, de elektronische snelweg enerzijds en het grote belang van een goede bescherming van de grondrechten van de burger anderzijds, vragen om een nauwgezette wettelijke regeling van de opsporingsbevoegdheden.
- Bij de nadere vormgeving van de opsporingsbevoegdheden dient een afweging plaats te vinden tussen het belang dat met opsporing is gediend en de kosten die de opsporingsfaciliteiten rond de elektronische snelweg met zich mee brengen, zowel voor de aanbieders en afnemers van elektronische diensten en producten als voor de overheid zelf.
- Internationale verdragen en samenwerkingsverbanden zijn onontbeerlijk voor uitoefening van rechtsmacht op de elektronische snelweg. Waar mogelijk dient harmonisatie van materiële normen te worden nagestreefd. Veelal zal dit geen geschikt of geen haalbaar instrument zijn en zal moeten worden gekozen voor minder vergaande oplossingen in de sfeer van bijvoorbeeld samenwerking tussen autoriteiten of het verlenen van rechtshulp.

Meer ten algemene wordt de wetgever met een lastig dilemma geconfronteerd. De grote technologische turbulentie en de grote diversiteit aan toepassingen en maatschappelijke omstandigheden vraagt om regelgeving die flexibel is en niet voor elke nieuwe techniek of toepassing hoeft te worden aangepast. Het proces van wetgeving duurt echter vaak dermate lang dat techniekspecifieke regels soms al verouderd zijn wanneer ze in werking treden. Dit speelt in het bijzonder bij formele wetten en bij de Grondwet. Om dit te voorkomen dient regelgeving liefst technologie-onafhankelijk te zijn, danwel zeer snel aanpasbaar.
Deze eisen staan echter op gespannen voet met de rechtsstatelijke eisen van legaliteit en rechtszekerheid. Een zekere mate van technische specificatie zit onherroepelijk in elke materiële normstelling opgesloten omdat men veelal het object van normstelling zal moeten benoemen.

Bovendien zal men rechtssubjecten de nodige houvast moeten geven over de aard van hun rechten en plichten en over de voorwaarden waaronder de overheid op die rechten inbreuk mag maken. De rechtszekerheid vraagt derhalve vaak om een zekere mate van technische specificiteit en continuïteit. Volledige technologie-onafhankelijke regelgeving zal daardoor in de praktijk in veel gevallen een illusie zijn.

In veel gevallen zal flexibele, technologie-onafhankelijke regelgeving nodig zijn om het hoofd te kunnen bieden aan de technologische turbulentie die zich thans rond de elektronische snelweg voordoet. Steeds zal daarbij echter wel een afweging moeten plaatsvinden met het belang van de rechtszekerheid voor de justitiabele. In Deel IV van deze nota wordt één en ander nader uitgewerkt.

DEEL IV TOETSINGSKADER

A. DE LEGITIMATIE VAN HET OVERHEIDSOPTREDEN

1. Een terughoudende opstelling

Nederland bevindt zich in de overgang naar een informatiesamenleving. Deel II B van deze nota identificeert drie kenmerken van die overgang die van bijzonder belang zijn voor een nadere plaatsbepaling van de rol van de overheid: dematerialisering, internationalisering en technologische turbulentie.

Deze fundamentele kenmerken hebben allereerst gevolgen voor de legitimatie van het overheidsoptreden, «mag de overheid optreden»? Hierbij houdt het kabinet uiteraard ook rekening met de sinds de jaren tachtig in de meeste westerse landen bestaande politieke en maatschappelijke context, waarbij overheden zich veelal beperken tot ordening. Privatisering, deregulering en marktwerking zullen op dit vlak voorlopig belangrijke motto's blijven.
De technologische turbulentie en ook de hoge omloopsnelheid van maatschappelijke problemen maken het voor een centrale, sturende actor zoals de nationale overheid moeilijk om adequaat en op tijd te handelen. Het is lastig om telkens voldoende inzicht te krijgen in de aard van de problemen en in de consequenties van de mogelijke oplossingen. Dematerialisering en internationalisering maken dat de overheid, zelfs waar zij wel een adequaat inzicht heeft, veelal maar een beperkte macht heeft om de ontwikkelingen zelfstandig te sturen. Nieuwe ontwikkelingen zullen veelal hun oorsprong vinden buiten de landsgrenzen. Dit noopt tot onderhandelingen met een reeks van internationale partners.
De mate en de aard van het overheidsoptreden zal echter sterk afhankelijk zijn van de vlucht die de elektronische snelweg neemt. Deze nota gaat uit van een niveau van «nevenschikking», waarin elektronische diensten een grote maatschappelijk en economische betekenis hebben, maar waarin geen *verdringing* van traditionele middelen plaatsvindt.
Hier geldt het aloude beginsel van «caveat emptor»: gebruikers zijn zelf verantwoordelijk voor hun keuzes. Men mag verwachten dat de markt in beginsel zijn werk zal doen en dat onbetrouwbare aanbieders en diensten vanzelf gemeden zullen worden. In de meeste westerse landen stelt de overheid zich daarom, zowel op nationaal als op supranationaal niveau, op het standpunt dat de ontwikkeling van de informatiesamenleving in beginsel aan de maatschappelijke krachten moet worden overgelaten.

Deze terughoudende opstelling betekent zeker niet dat er geen rol voor de overheid is weggelegd. Zij dient de verdere ontwikkeling van de informatiesamenleving zoveel mogelijk te stimuleren door zo gunstig mogelijke randvoorwaarden te scheppen. Zij acht het niet haar primaire taak om zelf een infrastructuur te realiseren. Dit betekent dat in het bijzonder de ordenende functie van de overheid in de informatiesamenleving van zeer groot belang zal zijn. Deel II B van deze nota gaat hier meer uitgebreid op in.

2. Twee hoofdtaken voor de overheid

Een en ander impliceert dat de overheid in de informatiesamenleving op korte termijn twee hoofdtaken in uitvoering moet nemen.

1. Het waarborgen van een aantal fundamentele normen en waarden van de democratische rechtsstaat in de elektronische omgeving.

Deze hoofdtaak wordt onderscheiden in:
- de bescherming en regeling van grondrechten, zoals privacy, briefgeheim en vrije meningsuiting,

- het verzekeren van rechtshandhaving op de elektronische snelweg en
- het bieden van rechtszekerheid.

2. Het faciliteren van het elektronisch maatschappelijk verkeer.

Deze hoofdtaak wordt onderscheiden in:
- het bevorderen van marktwerking,
- het bevorderen van de betrouwbaarheid van het elektronisch verkeer,
- het wegnemen van belemmeringen in de bestaande juridische infrastructuur en
- het stimuleren van ondersteunende voorzieningen, zoals TTP's en standaardisatie.

Uitgangspunt bij de uitvoering van beide hoofdtaken is dat de juridische waarden en normen uit de fysieke omgeving toepasbaar moeten zijn op de elektronische omgeving.
Burgers moeten ervan op aan kunnen dat hun rechten ook op de elektronische snelweg van toepassing zijn en dat zij er beschermd worden tegen misdrijven en andere inbreuken op hun rechten. In de informatiesamenleving is dit extra van belang, omdat een aantal fysieke zekerheden door de dematerialisering vermindert.
Voor een verdere ontwikkeling van het elektronisch maatschappelijk verkeer moeten er on-line en off-line zoveel mogelijk dezelfde normen gelden. Burgers en bedrijven moeten soepel kunnen switchen tussen traditionele en elektronische communicatie.

Daarnaast kan vooral de faciliterende taak mee brengen dat de overheid zelf initiatieven neemt. Het gaat hierbij bijvoorbeeld om:
- het bieden van voorzieningen, die de door de markt te realiseren infrastructuur ondersteunen,
- experimenten en pilotprojecten,
- subsidieverlening en
- het ondersteunen, of zelfs opleggen van standaardisatie.

Voor een deel is deze taak beschreven in Deel III D, voor een ander deel vallen die initiatieven buiten de reikwijdte van deze nota, die zich immers op het juridische instrumentarium richt.

3. Een derde hoofdtaak

De overheid heeft nog een derde hoofdtaak, die op dit moment echter nog niet leidt tot de inzet van juridisch instrumentarium:

3. Het garanderen van de elementaire voorzieningen die nodig zijn voor het maatschappelijk functioneren van burgers en bedrijven in een informatiesamenleving.

4. Wat betekent verdringing voor de rol van de overheid?

Mocht in de toekomst op bepaalde terreinen sprake zijn van een niveau van ontwikkeling waarbij elektronisch verkeer de traditionele vormen van communicatie verdringt, dan kan hoogstwaarschijnlijk niet worden volstaan met het vertalen van traditionele normen en kaders, die veelal voor de fysieke wereld zijn ontwikkeld. Dan zal moeten worden overwogen of geheel nieuwe normen en kaders nodig zijn, die speciaal worden ontwikkeld voor het elektronische domein.

Omdat burgers en bedrijven voor hun maatschappelijk functioneren bij verdringing afhankelijk worden van de elektronische snelweg, zal de overheid een brede toegankelijkheid van communicatievoorzieningen

moeten garanderen. Zij zal dan uitvoering moeten geven aan haar derde hoofdtaak, veelal door de inzet van juridische instrumenten.
De invulling van deze derde hoofdtaak hangt af van de omstandigheden. Soms kan de overheid volstaan met ordening in de sfeer van mededingings- of prijsbeleid. Soms zal specifieke wetgeving nodig zijn om de toegang tot bepaalde voorzieningen te verzekeren, of de pluriformiteit van meningsuitingen te garanderen. Deze taak komt voor een belangrijk deel overeen met de taak die is beschreven bij het thema «markten».

Samengevat luiden de legitimatiegronden voor overheidsoptreden als volgt:

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

B. PROBLEMEN VAN REGELGEVING

Als is vastgesteld dat er een taak voor de overheid is, gaat het vervolgens om het in te zetten instrumentarium. De eerdere delen van deze nota leiden tot de conclusie dat de overheid bij de vervulling van haar taken niet altijd kan vertrouwen op het klassieke wetgevingsinstrumentarium.

Samengevat:
Dematerialisering beïnvloedt:
- Transport en opslag: er is op de elektronische snelweg geen vanzelfsprekend onderscheid meer tussen transport en opslag van gegevens.
- Authenticiteit: gegevens op de elektronische snelweg kunnen perfect en onbeperkt worden gekopieerd. Gemanipuleerde gegevens en informatie zijn met de menselijke zintuigen niet van echt te onderscheiden.
- Anonimiteit versus kenbaarheid: moderne communicatiemiddelen en informatietechnieken dringen diep door in de persoonlijke levenssfeer. Kennis van de wederpartij is daarom een groot goed. Dit botst echter met traditionele uitgangspunten van anonimiteit en privacy.
- Open en besloten communicatie: het onderscheid tussen open en besloten vormen van communicatie is niet meer vanzelfsprekend. Dit vraagt nieuwe invullingen van belangrijke grondrechten, zoals privacy, brief- en telefoongeheim en de vrijheid van meningsuiting.

Internationalisering wordt behandeld in Deel III B, aan de hand van drie problemen voor de wetgever:
- Botsing van rechtsmacht. Naast de Nederlandse overheid zijn er soms nog een aantal andere nationale overheden die rechtsmacht over een handeling kunnen claimen.
- Het uiteenlopen van materiële normen. De materieelrechtelijke bepalingen verschillen vaak per land. Een handeling die in het ene land is toegestaan, kan tegelijkertijd in een ander land een strafbaar feit betekenen.
- Moeizame handhaafbaarheid. Handhaving van het recht is niet goed mogelijk wanneer het rechtssubject zich buiten de Nederlandse rechtssfeer bevindt, of wanneer zijn identiteit niet goed is vast te stellen.

Technologische turbulentie heeft gevolgen voor:
- Technologie-afhankelijkheid: door de snelle opeenvolging en convergentie van technieken en media biedt regelgeving op basis van concrete media of technieken op langere termijn onvoldoende houvast. Dit kan ook leiden tot rechtsongelijkheid tussen het gebruik van oude en nieuwe technieken en tot discrepanties tussen de on- en off-line communicatie.
- Flexibiliteit: het proces van formele wetgeving vergt zorgvuldige besluitvorming. Het kan daardoor te lang duren om de omloopsnelheid van problemen bij te benen. Wetgeving dreigt reeds te verouderen voor zij de Staatscourant bereikt;
- Adequaatheid: de wetgever ontbeert veelal de technische expertise en het inzicht in de maatschappelijke toepassingen van de techniek om op voorhand terreinen te kunnen reguleren.

De laatste twee problemen zijn op zichzelf niet nieuw. Internationalisering is ook op andere terreinen aan de orde. Ook zag de wetgever zich al eerder met technologische turbulenties geconfronteerd. Maar rondom de elektronische snelweg is de schaal waarop en de mate waarin deze problemen zich thans voordoen buitengewoon groot, evenals de maatschappelijke consequenties en politieke aandacht. Bovendien lijken

ze, net als de dematerialisering, in de informatiesamenleving een structureel karakter te krijgen.
Deze ontwikkelingen stellen de geloofwaardigheid van de wetgever op de proef. Regelgeving dient immers duidelijk, uitvoerbaar en handhaafbaar te zijn. Door dematerialisering, internationalisering en technologische turbulentie staan deze rechtsstatelijke eisen onder druk.

Deze nota gaat daarom uit van de behoefte aan flexibiliteit bij het optreden van de wetgever. Aan de andere kant zal de rechtszekerheid – zeker in een turbulente periode – vaak duidelijkheid van de wetgever verwachten. Bij oplossingen zal dit dilemma steeds in het oog moeten worden gehouden, waarbij de noodzaak tot flexibiliteit vaak toch bepalend zal zijn. Flexibel ingrijpen is dan de enige manier om nog te kunnen ingrijpen.

C. AANDACHTSPUNTEN VOOR REGELGEVING

Aanwijzing 6 van de Aanwijzingen voor de regelgeving luidt als volgt: tot het tot stand brengen van nieuwe regelingen wordt alleen besloten, indien de noodzaak daartoe is komen vast te staan. De noodzaak tot regelgeving rond de elektronische snelweg zal gegrond zijn op één van de hoofdtaken van de overheid, zoals eerder in dit hoofdstuk geformuleerd.

Nadat de noodzaak om op te treden is komen vast te staan, volgt de keuze van het instrumentarium (Aanwijzing 7 van de Aanwijzingen voor de regelgeving).

1. Nationaal of internationaal?

Een eerste vraag betreft de schaal waarop tot regelgeving dient te worden over gegaan. Als algemeen uitgangspunt geldt ook hier dat regelgeving zoveel mogelijk dient aan te sluiten bij de schaal van de maatschappelijke problemen. In het licht van het internationale karakter van de uitoefening en handhaving van rechten rond de elektronische snelweg, zal vaststelling van regels op supranationaal niveau vrijwel steeds het meest geëigend zijn. De voorkeur gaat daarbij uit naar mondiale verdragen, of in ieder geval verdragen waarvan zoveel mogelijk landen partij worden.

Haalbaarheid en tijdigheid kunnen echter voor regelgeving op mondiaal niveau belangrijke obstakels zijn. Regeling binnen OESO of bijvoorbeeld de Raad van Europa, is dan een goed alternatief. Het is daarbij wel van belang de landen te betrekken die toonaangevend zijn op het gebied van informatie- en communicatietechnologie, zoals de Verenigde Staten. Als ook dat alternatief niet haalbaar is, wordt gekozen voor het niveau van de Europese Unie.

Ook zal de harmonisatie van materieelrechtelijke normen op mondiaal niveau soms onmogelijk of onwenselijk zijn, wanneer de culturele en maatschappelijke opvattingen te zeer uiteenlopen.

Onder de volgende omstandigheden is een keuze voor nationale wetgeving gerechtvaardigd:

- Indien het nodig is ter bescherming van fundamentele normen en waarden.
- Indien regeling op een hoger niveau niet haalbaar is of te lang zou duren.
- Indien het beoogt de concurrentiepositie van Nederland te versterken.
- Als voorbeeldfunctie voor de internationale rechtsontwikkeling.

Nationale ordening is echter alleen zinvol indien deze ook door de Nederlandse autoriteiten of justitiabelen handhaafbaar is. Zie hiervoor ook: Aanwijzingen voor de regelgeving, Aanwijzing 11.

2. Zelfregulering of overheidsregulering?

De Aanwijzingen voor de regelgeving hebben als uitgangspunt dat overheidsingrijpen slechts op zijn plaats is indien de noodzaak van interventie kan worden aangetoond en indien van het zelfregulerend vermogen van de betrokken maatschappelijke partijen onvoldoende resultaten zijn te verwachten. Zie hiervoor bijlage 6 van deze nota. Dematerialisering, internationalisering en technologische turbulentie geven dit uitgangspunt voor de elektronische omgeving extra gewicht. In een zich snel wijzigende en technisch complexe en internationale omgeving beschikken maatschappelijke partijen soms over meer expertise en inzicht in de aard van de problemen en de haalbaarheid en

adequaatheid van mogelijke oplossingen, dan een relatieve buitenstaander zoals de overheid. Bovendien is zelfregulering niet gebonden aan territoriale grenzen van staten.

Zelfopgelegde vormen van regulering door de betrokken partijen verdienen de voorkeur boven wetgeving. Zelfregulering kan bestaan uit algemene, privaatrechtelijke afspraken tussen en op initiatief van aanbieders en gebruikers van ICT-diensten en producten. Daarbij kan men denken aan standaardclausules in gebruikerscontracten, algemene leveringsvoorwaarden, gebruikersprotocollen en onderlinge vormen van certificering en normalisatie. Ook is het voor te stellen dat men, eventueel internationale, arbitrageregelingen treft.
Er bestaat een uitzondering op de voorkeur voor zelfregulering. Zelfregulering als alternatief voor overheidsregulering is niet geschikt indien fundamentele normen en waarden van de democratische rechtsstaat in het geding zijn. In het geval van de elektronische snelweg kan men daarbij vooral denken aan bescherming van klassieke grondrechten van burgers en aan de preventie en opsporing van inbreuken op de rechtsorde en de staatsveiligheid. In deze gevallen zal niet kunnen worden volstaan met onderlinge afspraken tussen partijen, maar zal wetgeving nodig zijn. Dit neemt niet weg dat de concretisering van die wetgeving heel goed met behulp van zelfregulering tot stand kan komen.

Zelfregulering zal, om aanvaardbaar te zijn als alternatief voor overheidsregulering, aan de volgende elementaire voorwaarden moeten voldoen:
- De doelgroepen die in het geding zijn, zijn voldoende georganiseerd.
- Er vindt een gelijkwaardige behartiging van de maatschappelijke belangen plaats.
- Er vindt voldoende binding plaats van alle partijen.
- De handhaving van de afspraken is voldoende verzekerd.

Deze set van voorwaarden verschilt niet wezenlijk van de eisen die men ook buiten de elektronische snelweg aan zelfregulering stelt. Op de elektronische snelweg kan met name het internationale karakter van markten het vervullen van deze voorwaarden soms extra moeilijk maken. Zo is rond Internet, met zijn wereldomspannende karakter, het risico van vrijhavens bijzonder groot.

Het is de taak van de overheid om er voor te zorgen dat deze voorwaarden worden nageleefd. Voor de uitvoering van deze taak zijn onder meer de volgende instrumenten geschikt:
- Het behartigen van onvoldoende vertegenwoordigde – kwetsbare – belangen.
- Het opstellen van ondersteunende wetgeving, zoals het onder omstandigheden toekennen van bewijskracht aan arrangementen die door zelfregulering tot stond is gekomen. Het neerleggen van naar tevredenheid werkende zelfregulering in een standaardregeling als bedoeld in artikel 6:124 BW, is hiervan tevens een voorbeeld.
- Het dreigen met wetgeving, indien de zelfregulering niet aan de voorwaarden voldoet
- Het houden van toezicht op de zelfregulering
- Het meewerken aan de handhaving van de zelfregulering, zoals dit nu al gebeurt bij het Internet Meldpunt Kinderporno.

Steeds zal moeten worden overwogen welke instrumenten de voorkeur verdienen.

Tot slot: Op langere termijn kan er juist wel weer reden zijn voor overheidsregulering. Dit kan het geval zijn, indien:
- Er sprake is van een niveau van ontwikkeling waarbij verdringing plaatsvindt. De overheid dient dan garanties te scheppen voor de toegankelijkheid.

- De technologische turbulentie afneemt en een periode van stabiliteit aanbreekt. Ter bevordering van de rechtszekerheid zou dan ook codificatie kunnen plaatsvinden van via zelfregulering ontstane normen.

3. Rechter, bestuur of wetgever?

Indien eenmaal is vastgesteld dat overheidsoptreden op zijn plaats is, luidt de derde vraag welke vorm dit dient aan te nemen. Ook hier vormen de reeds genoemde Aanwijzingen 6 t/m 8 het uitgangspunt. Dit overheidsingrijpen dient zo flexibel, adequaat en tijdig mogelijk te zijn. Aan de andere kant moet het overheidsingrijpen ook voldoende rechtszekerheid bieden. Het spreekt voor zich dat deze beide vereisten met elkaar kunnen conflicteren. Er dient dan een rationele afweging plaats te vinden.

3.1. Getoetst wordt of de rechtsontwikkeling niet aan de rechter kan worden overgelaten.

De rechter past bestaande normen uit de fysieke wereld toe in de elektronische omgeving. Algemene normen uit het privaatrecht, maar ook andere technologie-onafhankelijke regels lenen zich hiervoor.
Indien de bestaande wettelijke normen op deze gebieden voldoende houvast bieden voor de rechter, heeft het kabinet de voorkeur de rechtsontwikkeling aan de rechter over te laten. Die is immers in staat op snelle en adequate wijze te reageren op verschijnselen in de elektronische omgeving. Aan de andere kant stelt juist het wezenlijk nieuwe karakter van de elektronische snelweg eisen aan de rechtszekerheid en aan de wettelijke regels.
Hierbij spelen de volgende afwegingen een rol:

- Biedt het bestaande juridisch instrumentarium voldoende houvast? In het bijzonder: hebben de bestaande normen een zekere universele geldende waarde en toepasbaarheid?
- Heeft optreden van de wetgever een toegevoegde waarde, bijvoorbeeld uit oogpunt van rechtszekerheid, of ter uitoefening van de faciliterende rol van de overheid?
- Gaat het om het waarborgen van grondrechten, of om de rechtshandhavingstaak van de overheid, waarvoor de wetgever de rechtsontwikkeling ter hand moet nemen?

3.2. Getoetst wordt of overheidsoptreden langs bestuurlijke weg kan plaatsvinden.

Bij die bestuurlijke weg gaat het om de volgende alternatieven:

- Een voorbeeldfunctie als gebruiker van de elektronische snelweg: de zogeheten «Parador-strategie». Het bestuur kan als dominante marktpartij een belangrijke voorbeeldfunctie vervullen. De Nederlandse overheid heeft deze «Paradorstrategie» in de periode van de wederopbouw toegepast op het terrein van de volkshuisvesting. De overheid stelt als grootafnemer van ICT zelf hoge eisen in de contracten die zij voor eigen gebruik afsluit met aanbieders van ICT, in de hoop dat deze als algemene standaard door de markt zullen worden overgenomen. Zo stelt deze nota voor om bij de inrichting van haar informatiesystemen de privacy te stimuleren door zelf voorop te lopen bij het gebruik van privacy enhancing technologies, PET's.
- Voorlichting aan consumenten over de mogelijkheden en risico's van ICT-diensten en producten. Zo kan de overheid het publiek wijzen op de privacy-risico's van transacties via Internet, of ouders oproepen voorzieningen te treffen om kinderen af te schermen van gewelddadige beelden.
- Convenanten. Het bestuur kan met private partijen afspraken maken

over gedragsregels. De Aanwijzingen voor convenanten bieden een kader voor convenanten, die de Rijksoverheid aangaat. Een recent voorbeeld hiervan zijn de richtlijnen van de Raad van Europa voor de bescherming van privacy op Internet. Deze zijn bedoeld als basis voor de ontwikkeling van een gedragscode voor Internetproviders. In Nederland biedt de procedure bij de Raad voor Accreditatie en Certificatie bijvoorbeeld ook mogelijkheden om specifieke overheidsbelangen bij de certificatie van instellingen en bedrijven mee te wegen. In deze nota wordt aanbevolen een kader te scheppen voor de activiteiten van TTP's.

3.3. Getoetst wordt of een nadere uitwerking van het privaatrecht, met het oog op de elektronische snelweg geschikt is.

De wetgever beperkt zich in deze strategie tot het in de privaatrechtelijke sfeer creëren van algemene waarborgen voor deelnemers aan het elektronisch rechtsverkeer. Steeds wordt nagegaan of het probleem niet kan worden opgelost door nadere invulling of uitwerking van de bestaande privaatrechtelijke wetgeving, specifiek voor die situaties, die zich op de elektronische snelweg voordoen. Zo zou de aansprakelijkheid van deelnemers aan het elektronisch rechtsverkeer nader kunnen worden gereguleerd door wetgeving die voor on-line situaties een nadere invulling geeft aan de bestaande regeling. Dit geldt zowel voor tekortkomingen in de nakoming van een verbintenis, als voor de onrechtmatige daad. Aldus zou de mate van zorg die in een elektronische omgeving jegens de wederpartij of een derde dient te worden betracht, kunnen worden verduidelijkt.
Voorts stelt deze nota voor om in het Burgerlijk Wetboek een aantal algemene bepalingen op te nemen, als leidraad voor de rechter bij het vormgeven van de rechtsontwikkeling. Het zou dan gaan om bepalingen vergelijkbaar met de zogenaamde «kapstokbepalingen» over goede trouw, redelijkheid en billijkheid en uitoefening van privaatrechtelijke bevoegdheden in strijd met publiekrecht.

Het kabinet acht het privaatrecht derhalve van groot belang voor het regelen van onzekere rechtsverhoudingen op de elektronische snelweg. Twee punten van afweging:
- Het verdient aanbeveling de regeling van de aansprakelijkheid op internationaal niveau vast te leggen. In ieder geval kan de Nederlandse regelgeving op dit punt niet te zeer afwijken van wat internationaal gebruikelijk is.
- De noodzaak en omvang van de consumentenbescherming in de elektronische omgeving vergt vaak aparte aandacht.

3.4. Indien geen van de voorgaande opties voldoende geschikt is, wordt gekozen voor publiekrechtelijke wetgeving.

Daarbij wordt gezocht naar alternatieven voor gedetailleerde normstelling, waarbij ook hier de afweging tussen rechtszekerheid en flexibiliteit centraal staat. Het heeft de voorkeur in de formele wetgeving algemene normen op te nemen. Gedetailleerde normstelling op het niveau van de wet is evenwel nodig, indien:
- meer specifieke normen nodig zijn om de bescherming van klassieke grondrechten te verzekeren en
- de voorwaarden worden vastgelegd, waaronder de overheid op die rechten inbreuk mag maken.

Een en ander doet overigens geen afbreuk aan het primaat van de wetgever, zoals verwoord in Aanwijzing 22 van de Aanwijzingen voor de regelgeving.

Voorts heeft het kabinet een voorkeur voor technologie-onafhankelijke wetgeving. Evenwel: technologie-afhankelijkheid kan nodig zijn:
- voor de vaststelling van het object van de regeling,
- om houvast te geven over de aard van de rechten en plichten die de regeling meebrengt en
- voor de vaststelling van de voorwaarden waaronder de overheid inbreuk kan maken op de rechten.

De voorkeur voor technologie-onafhankelijke wetgeving kan er toe leiden inhoudelijke normen niet op te nemen in specifieke, technische wetgeving. Ter toelichting bijvoorbeeld alle regels over privacy in een algemene privacywet en niet in verschillende op technologie gebaseerde sectorspecifieke wetten.

Invulling van de algemene normen uit de wet kan plaatsvinden door:
- Zelfregulering. Bij deze hybride vorm van regulering neemt de wetgever het initiatief en stelt hij zelf de kaders vast waarbinnen de zelfregulering moet geschieden. Bijvoorbeeld: alleen de nadere technische invulling wordt overgelaten aan marktpartijen en private normalisatieinstituten. Voor zover deze geconditioneerde zelfregulering strekt tot nadere invulling van overheidsverantwoordelijkheden, zullen er een aantal formele en procedurele eisen gelden. Deze zijn in de elektronische omgeving niet anders dan in de traditionele omgeving.
- De rechter. De wetgever onthoudt zich van het geven van concrete gedragsvoorschriften en technische detaillering.
- Een AMvB en/of een ministeriële regeling. Op zichzelf biedt de elektronische snelweg wat dit betreft niets nieuws, zij het dat de technologische turbulentie eerder gebruikmaking van deze instrumenten zal rechtvaardigen.
- Een mengvorm tussen de voorgaande alternatieven. Een voorbeeld daarvan is de constructie, waarbij de formele wetgever de bevoegdheid toekent een AMvB of een ministeriële regeling vast te stellen, tenzij inmiddels zelfregulering tot stand is gekomen. Nog verdergaand is het alternatief waarbij de wetgever bepaalde marktpartijen opdraagt zelfregulering tot stand te brengen. Mengvormen tussen overheidsregulering en zelfregulering kunnen in verschillende vormen voorkomen.

Er vindt steeds een rationele keuze plaats tussen deze drie alternatieven, met inachtneming van de eerder voor zelfregulering en rechtsvorming door de rechter gegeven aandachtspunten. Bij die keuze wordt ook steeds gekeken naar mogelijkheden van mengvormen tussen de drie alternatieven. Een mengvorm kan in specifieke situaties een zeer geschikt alternatief zijn.

Een alternatief, waarbij een toezichthoudende instantie open normen concretiseert, wordt niet in de afweging betrokken. Deze variant zou neerkomen op het toekennen van regelgevende bevoegdheid aan een toezichthouder – de uit de Verenigde Staten en het Verenigd Koninkrijk bekende «regulatorsfunctie». Dit past niet goed binnen het Nederlandse staatsrecht. Regelgevende bevoegdheid wordt niet gedelegeerd aan organen die niet rechtstreeks aan parlementaire controle zijn onderworpen.

D. HET TOETSINGSKADER ZELF

De aandachtspunten voor regelgeving leiden tot een toetsingskader.

Het toetsingskader is een hulpmiddel voor de actoren in het wetgevingsproces, dat hen in staat moet stellen consistente afwegingen te maken bij het voorbereiden en opstellen van regelgeving, die verband houdt met ontwikkelingen op het gebied van informatie- en communicatietechnologie. Meer in het bijzonder is het gericht op een goede motivering van gemaakte keuzes, zeker waar die keuzes afwijken van de in het kader genoemde hoofdregels.

Het toetsingskader wordt toegepast door diegene binnen de Rijksdienst die zijn belast met:
- De voorbereiding en vaststelling van regelingen.
- De voorbereiding en uitvoering van verdragen en van besluiten van volkenrechtelijke organisaties, waaronder de Europese Unie.

De toepassing van het toetsingskader maakt ook onderdeel uit van de reguliere toetsing van regelgeving, die op grond van Aanwijzing 254 van de Aanwijzingen voor de regelgeving wordt uitgevoerd door de Directie Wetgeving van het Ministerie van Justitie.
Ook andere actoren in het wetgevingsproces kunnen het toetsingskader toepassen.

De toelichting bij een regeling bevat een verslag van de toepassing van het toetsingskader.
Het toetsingskader is een hulpmiddel en leidt niet tot afdwingbare keuzes. Het kan dit ook niet hebben, gelet op de complexiteit van de te beantwoorden vragen. Bovendien is voor sommige vraagstukken niet een enkel specifiek instrument, maar juist een mix van de genoemde instrumenten het meest geschikt.

Het toetsingskader luidt als volgt.

1.1 Regelgeving dient bij voorkeur plaats te vinden op mondiaal niveau, of in ieder geval tezamen met zoveel mogelijk landen. Met name het privaatrecht leent zich daarvoor en voorts standaardisatie en andere regelgeving op het gebied van de economische ordening, maar ook andere onderwerpen waarover de culturele opvattingen niet sterk uiteenlopen.
Indien dit niet haalbaar is, is regeling in kleiner internationaal verband, zoals OESO of Raad van Europa, een goed alternatief. Indien dat alternatief ook niet haalbaar is, wordt gekozen voor het niveau van de Europese Unie.

1.2 Regelgeving op nationaal niveau kan worden overwogen:
- *ter bescherming van normen en waarden,*
- *indien regelgeving op internationaal niveau niet haalbaar is, of te lang zou duren,*
- *om de concurrentiepositie van Nederland te versterken, of*
- *als voorbeeldfunctie voor de internationale rechtsontwikkeling.*

2.1 Als alternatief voor overheidsregulering dient eerst te worden onderzocht of andere oplossingen mogelijk zijn, waarbij vormen van zelfregulering zoveel mogelijk moeten worden gestimuleerd. Dit geldt in ieder geval zolang:
- *geen «verdringing» van traditionele communicatie plaatsvindt en*
- *er sprake is van technologische turbulentie.*

Daarnaast kan voor problemen, veroorzaakt door technologie, in sommige gevallen de technologie zelf ook oplossingen aanreiken. Filtersystemen ter

bescherming van jeugdigen tegen ongewenst aanbod zijn hiervan een voorbeeld.

2.2 Deze zelfregulering dient aan de volgende voorwaarden te voldoen:
- *De doelgroepen die in het geding zijn, zijn voldoende georganiseerd.*
- *Er vindt er een gelijkwaardige behartiging plaats van de relevante maatschappelijke belangen.*
- *Er vindt voldoende binding plaats van alle partijen.*
- *De handhaving van de afspraken is voldoende verzekerd.*

2.3 De overheid draagt zorg voor de naleving van de voorwaarden genoemd onder 2.2. Zij kan daarvoor onder meer de volgende instrumenten gebruiken:
- *Het behartigen van onvoldoende vertegenwoordigde belangen.*
- *Het opstellen van ondersteunende wetgeving.*
- *Het dreigen met wetgeving, indien de zelfregulering niet aan de voorwaarden voldoet.*
- *Toezicht.*
- *Het meewerken aan de handhaving.*

2.4 Overheidsoptreden is in ieder geval aan de orde indien fundamentele normen en waarden van de democratische rechtsstaat in het geding zijn. Met betrekking tot de elektronische snelweg kan men daarbij vooral denken aan bescherming van klassieke grondrechten van burgers en aan de preventie en opsporing van ernstige inbreuken op de rechtsorde en de staatsveiligheid.

3.1 Vanwege het turbulente karakter van de ontwikkelingen rond de elektronische snelweg dient het overheidsingrijpen zo flexibel, adequaat en tijdig mogelijk te zijn. Afweging met het belang van de rechtszekerheid vindt plaats.

3.2 Het wordt getoetst of bestaande wettelijke normen voldoende houvast bieden, zodat de rechtsontwikkeling aan de rechter kan worden overgelaten.

3.3 Het wordt getoetst of overheidsoptreden langs bestuurlijke weg kan plaatsvinden. Daarbij kan men denken aan:
- *een voorbeeldfunctie als gebruiker van de elektronische snelweg,*
- *voorlichting en*
- *convenanten.*

Voor zover dit bestuurlijk optreden de vrijheid van particulieren beperkt, is daarvoor een wettelijke grondslag vereist.

3.4 Het wordt getoetst of een nadere uitwerking van het privaatrecht met het oog op de elektronische snelweg geschikt is, teneinde rechtsonzekerheid in rechtsverhoudingen weg te nemen.

3.5 Indien geen van de voorgaande vormen, of een combinatie daarvan, voldoet, zal het overheidsingrijpen echter plaats dienen te vinden in de vorm van, of binnen het kader van, formele, publiekrechtelijke wetgeving. Daarbij wordt gezocht naar alternatieven voor materiële normen in de wet. De formele wet omvat alleen algemene normen, tenzij:
- *meer specifieke normen nodig zijn om de bescherming van klassieke grondrechten te verzekeren, of*
- *de voorwaarden worden vastgelegd waaronder de overheid op die rechten inbreuk mag maken.*

3.6 Getoetst wordt of technologie-onafhankelijke regelgeving mogelijk is. Technologie-onafhankelijke regels zijn niet geschikt:

- *als definitie van de reikwijdte van een regeling;*
- *als rechtssubjecten – in verband met de ingewikkelde technologie – juist behoefte hebben aan inzicht in de technologie;*
- *als technologie-onafhankelijke regels aan rechtssubjecten onvoldoende houvast zouden bieden over de aard van hun rechten en plichten, of*
- *de voorwaarden worden vastgelegd, waaronder de overheid op die rechten inbreuk mag maken.*

De voorkeur voor technologie-onafhankelijke wetgeving kan er toe leiden inhoudelijke normen niet op te nemen in specifieke, technische wetgeving. Ter toelichting: bijvoorbeeld alle regels over privacy worden opgenomen in een algemene privacywet en niet in verschillende op technologie gebaseerde sectorspecifieke wetten.

3.7 Bij de invulling van algemene normen wordt een keuze gemaakt tussen:

- *zelfregulering,*
- *overlaten aan de rechter en*
- *een AMvB, of een ministeriële regeling en*
- *een mengvorm tussen de voorgaande instrumenten.*

DEEL V ACTIEPUNTEN

A. INLEIDING

Dit deel van de nota ziet op de implementatie van de voorstellen uit de nota.

Ter herinnering: de nota levert twee producten op:
1. een gemeenschappelijk toetsingskader voor het kabinet bij vragen van wetgeving rond de elektronische snelweg;
2. voorstellen voor het opstellen, aanpassen of intrekken van wetgeving en voor de inbreng in internationale overlegfora, of voor daarmee samenhangende activiteiten.

Het toetsingskader kan met onmiddellijke ingang worden toegepast, zij het dat het aanbeveling verdient het toetsingskader te verankeren in de Aanwijzingen voor de regelgeving. Voor de overige voorstellen geldt dit niet. De implementatie daarvan zal gefaseerd ter hand worden genomen, overeenkomstig het onderstaande actieplan.

Binnenkort zal de Tweede Kamer worden geïnformeerd over een tweede Nationaal Actieprogramma Elektronische Snelwegen. De besluitvorming daaromtrent zal naar verwachting ten behoeve van de Kabinetsformatie plaatsvinden. Zo mogelijk worden de voorstellen van deze nota in het tweede actieprogramma opgenomen. Het is gewenst dat de voortgangsbewaking van de implementatie van deze nota in dat actieprogramma wordt ingebed.

Tot slot wordt op deze plaats nog de aandacht gevestigd op het regelmatige overleg dat het Ministerie van Justitie bij de voorbereiding van de nota heeft gevoerd met deskundigen bij het belanghebbende bedrijfsleven in een expertisegroep. Dit overleg is wederzijds goed bevallen en zal worden voortgezet ter voorbereiding van niet alleen de uitvoering van de voorstellen uit dit actieplan, maar ook voor andere werkzaamheden waarvoor het overleg met het bedrijfsleven dienstig is.

B. HET TOETSINGSKADER

Het toetsingskader wordt toegepast door diegene binnen de Rijksdienst die zijn belast met:
- de voorbereiding en vaststelling van regelingen,
- de voorbereiding en uitvoering van verdragen en van besluiten van volkenrechtelijke organisaties, waaronder de Europese Unie.

De toepassing van het toetsingskader maakt ook onderdeel uit van de reguliere toetsing van regelgeving, die op grond van Aanwijzing 254 van de Aanwijzingen voor de regelgeving wordt uitgevoerd door de Directie Wetgeving van het Ministerie van Justitie.

Het verdient aanbeveling het toetsingskader te verankeren in de Aanwijzingen voor de regelgeving, door in een nieuw te formuleren aanwijzing naar het toetsingskader te verwijzen. Met deze verankering wordt bewerkstelligd dat het toetsingskader ook op langere termijn gehanteerd blijft worden.
Aan de Interdepartementale Commissie voor de Harmonisatie van Wetgeving wordt verzocht dit onderwerp mee te nemen bij de eerstvolgende wijziging van de Aanwijzingen voor de regelgeving en daarbij tevens advies uit te brengen over de inhoud van de nieuw te formuleren aanwijzing.

C. IMPLEMENTATIE VAN DE OVERIGE VOORSTELLEN

In de implementatiefase worden de voorstellen van de nota geclusterd in een aantal projecten en deelprojecten. De uitvoering hiervan zal plaats vinden binnen de normale organisatiestructuur van de betrokken departementen. Er wordt geen nieuwe (overkoepelende) projectstructuur in het leven geroepen.
De bij de verschillende projecten genoemde bewindslieden zijn verantwoordelijk voor de voortgang van de implementatie. Wel zal worden voorzien in een voortgangsbewaking, te coördineren door de Minister van Justitie, zo mogelijk binnen het kader van een tweede Nationaal Actieprogramma elektronische snelwegen. Het is gewenst dat:

- de primair verantwoordelijken regelmatig in werkgroepverband bijeenkomen, teneinde een goede informatie-uitwisseling te garanderen;
- de voortgangsbewaking leidt tot een eerste voortgangsrapportage die op 1 april 1999 plaatsvindt.

Voor de implementatie van de nota is een actieplan opgesteld.
Het actieplan geeft per project (en per deelproject) het volgende aan:

- beoogd resultaat;
- omschrijving van de te ondernemen activiteiten;
  Soms worden daarbij tussenstappen aangegeven
- samenhang met andere voorstellen en met de belangrijkste conclusies van de nota;
  Ook: het belang van het voorstel voor de implementatie van de nota
- prioriteit en beoogd tijdpad;
- wie is verantwoordelijk voor de implementatie?

Het is raadzaam dat het volgende kabinet na twee jaar beziet in hoeverre deze nota nog actueel is. Dan kan ook besluitvorming plaatsvinden over de voorstellen, waarvan de uitvoering afhangt van:

- de technologische ontwikkelingen;
- het niveau van ontwikkeling van de elektronische snelweg, waarbij de verhouding tussen nieuwe en tradtionele media als meetpunt dient.

Deze voorstellen zijn ter informatie aan het plan van aanpak toegevoegd. De actualisering kan gelijktijdig met de tweede voortgangsrapportage in begin 2000 plaatsvinden.

D. ACTIEPLAN

Het actieplan bestaat uit de volgende projecten:

1. Privaatrecht
2. Strafrecht (wetgeving)
3. Strafrechtelijke handhaving
4. Bestuursrecht
5. Communicatie met de overheid
6. Privacy
7. Vrijheid van meningsuiting
8. Biometrie en identificatie
9. Trusted Third Parties
10. Marktwerking
11. Internationalisering en rechtsmacht (nationale uitvoering)
12. Internationalisering en rechtsmacht (inbreng in internationale gremia)
13. Toegevoegd project: actualisering nota (begin 2000).

De voortgangsbewaking wordt opgedragen aan de Directie Wetgeving van het Ministerie van Justitie.

In het actieplan zijn enkele deelprojecten gekenschetst als bepalend voor de implementatie van de nota. Deze deelprojecten zullen in het implementatietraject als speerpunt gelden. De deelprojecten zijn: 1.1, 1.2, 2.1, 9.1, 12.1, 12.2 en 12.3.

1. Privaatrecht

1. In het Burgerlijk Wetboek worden algemene bepalingen opgenomen, die de rechter houvast geven bij de toepassing van het vermogensrecht op de elektronische snelweg.

Beoogd resultaat:	indiening wetsvoorstel.
Omschrijving activ.:	normaal wetgevingsproces.
Samenhang:	bepalend voor implementatie nota (invulling aan faciliterende taak overheid)/hangt samen met o.a. 1.2, (deels) 8 en (deels) 9.
Prioriteit:	hoog, aanvang werkzaamheden 1e helft 1998, streefdatum indiening medio 1999.
Verantwoordelijk:	Ministerie van Justitie.

2. Bezien wordt of bij concreet gebleken wettelijke belemmeringen voor het elektronisch rechtsverkeer deze moeten en kunnen worden opgeheven.

Beoogd resultaat:	indiening wetsvoorstel(len).
Omschrijving activ.:	normaal wetgevingsproces.
Samenhang:	bepalend voor implementatie nota (invulling aan faciliterende taak overheid)/hangt samen met o.a. 1.1.
Prioriteit:	hoog, afhankelijk vanaf het moment dat belemmeringen zich voordoen.
Verantwoordelijk:	Ministerie van Justitie.

3. Het kabinet zal bevorderen dat zelfregulering tot stand komt over elektronische pseudo-koop en andere vormen van misleiding van consumenten langs elektronische weg.

Beoogd resultaat:	totstandkomen zelfregulering, die aan waarborgen uit toetsingskader voldoet.
Omschrijving activ.:	initiëren overleg met de Consumentenbond en de brancheorganisaties in de sfeer van de reclame en telemarketing, evt. ondersteunen totstandbrengen zelfregulering.
Samenhang:	invulling aan faciliterende taak overheid, consumentenbescherming.
Prioriteit:	middel, aanvang werkzaamheden 2e helft 1998, streefdatum eindresultaat 2e helft 1999.
Verantwoordelijk:	Ministerie van Economische Zaken.

2. Strafrecht (wetgeving)

1. Het kabinet streeft er naar het Wetsvoorstel computercriminaliteit II nog in 1998 bij de Tweede Kamer in te dienen.

Beoogd resultaat:	indiening wetsvoorstel
Omschrijving activ.:	normaal wetgevingsproces (wetsvoorstel is reeds in consultatie).
Samenhang:	bepalend voor implementatie nota (o.a. aansprakelijkheid tussenpersoon).
Prioriteit:	hoog, streefdatum eindresultaat eind 1998.
Verantwoordelijk:	Ministerie van Justitie.

2. Onderzocht wordt of in het Wetboek van Strafvordering een bevoegdheid voor de rechter-commissaris moet worden opgenomen, die inhoudt dat in zwaarwegende gevallen over mag worden gegaan tot een algemene vergelijking van registers van verdachte en niet verdachte burgers.

Beoogd resultaat:	al dan niet noodzaak tot opnemen van deze bevoegdheid.
Omschrijving activ.:	verrichten van onderzoek.
Samenhang:	strafrechtelijke rechtshandhaving door toesnijden wetgeving op nieuwe technologie/samenhang met 31.
Prioriteit:	middel, aanvang onderzoek 1e helft 1998, resultaat 2e helft 1998.
Verantwoordelijk:	Ministerie van Justitie.

3. Op basis van de resultaten van het onderzoek van het WODC naar het verkrijgen van gegevens bij derden (fase I), wordt onderzocht in welke vorm in het Wetboek van Strafvordering een bevoegdheid wordt opgenomen die inhoudt dat een derde verplicht kan worden uit een door hem in stand gehouden persoonsregistratie een gegeven te verstrekken. Aan deze verplichting moet worden gekoppeld dat kan worden afgeweken van de normale privacy-regelgeving (fase II).

Beoogd resultaat:	fase I: onderzoeksresultaat als basis voor nationale besluitvorming; fase II: indiening wetsvoorstel.
Omschrijving activ.:	fase I: afronding onderzoek; fase II: normaal wetgevingsproces.
Samenhang:	strafrechtelijke rechtshandhaving /hangt samen met 3.4.
Prioriteit:	hoog, afhankelijk onderzoek WODC (rapportage verwacht voorjaar 1998).

	Fase 2: rapportage over invulling bevoegdheid opvragen persoonsgegevens bij derden 1e helft 1999; indiening wetsvoorstel eind 1999.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Verkeer & Waterstaat.

4. Ten behoeve van de bestrijding van de georganiseerde criminaliteit zal onderzoek worden verricht naar de mogelijkheid en wenselijkheid van het op verzoek van opsporingsinstanties vergaren van locatiegegevens door telecommunicatie-aanbieders en credit card maatschappijen. Het betreft dan gegevens die niet reeds worden vergaard in het kader van de eigen bedrijfsvoering van deze organisaties.

Beoogd resultaat:	inzicht verkrijgen in de mogelijkheden van de techniek ten behoeve van de opsporing van georganiseerde criminaliteit.
Omschrijving activ.:	verrichten van onderzoek.
Samenhang:	benutten van de techniek ten behoeve van de rechtshandhaving.
Prioriteit:	laag, aanvang onderzoek 1e helft 1999; rapportage 2e helft 1999.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Verkeer en Waterstaat.

5. Het kabinet zal bevorderen dat het stelsel van zelfregulering, zoals nu bestaat voor het Internet Meldpunt Kinderporno, wordt uitgebreid tot andere uitingsdelicten (Fase 1) en op termijn ook tot andere categorieën tussenpersonen (Fase 2).

Beoogd resultaat:	totstandkomen zelfregulering die aan waarborgen toetsingskader voldoet en waarborgen handhavingscapaciteit (Fase 1 en 2).
Omschrijving activ.:	initiëren overleg met de internetproviders, evt. ondersteunen totstandbrengen zelfregulering, capaciteit beschikbaar stellen voor de strafrechtelijke handhaving van de gemelde delicten.
Samenhang:	strafrechtelijke rechtshandhaving, effectieve wijze van optreden tegen uitingsdelicten.
Prioriteit:	Fase 1: hoog, aanvang werkzaamheden 1e helft 1998, streefdatum eindresultaat 1e helft 1999; Fase 2: laag, aanvang werkzaamheden 1e helft 1999.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Binnenlandse Zaken.

6. Onderzocht wordt of een aanpassing van artikel 350a van het Wetboek van Strafrecht is aangewezen.

Beoogd resultaat:	eventueel wetsvoorstel.
Omschrijving activ.:	uitvoering onderzoek.
Samenhang:	omdat vormen van manipulatie van stromende informatie technisch mogelijk zijn, kan het nodig zijn wetgeving toe te snijden op nieuwe technologie; betrouwbaarheid van elektronisch rechtsverkeer.
Prioriteit:	middel, aanvang werkzaamheden 2e helft 1998, streefdatum eindresultaat 1e helft 1999.
Verantwoordelijk:	Ministerie van Justitie.

7. Het kabinet streeft naar internationale afspraken over de opsporing en vervolging van elektronische vormen van bedrog. Hieraan voorafgaande

is onderzoek nodig naar de technische en maatschappelijke haalbaarheid van detectietechnieken.

Beoogd resultaat:	Fase 1: onderzoeksresultaat als basis voor internationale besluitvorming; Fase 2: aanvang internationale onderhandelingen.
Omschrijving activ.:	Fase 1: uitvoering onderzoek; Fase 2: initiëren internationaal overleg, in eerste instantie in het verband van de EU.
Samenhang:	strafrechtelijke rechtshandhaving/faciliteren betrouwbaar rechtsverkeer.
Prioriteit:	middel, Fase 1: aanvang werkzaamheden 1e helft 1999, streefdatum afronding medio 1999/Fase 2: aanvang werkzaamheden medio 1999.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Binnenlandse Zaken.

3. Strafrechtelijke handhaving

1. Onderzoek vindt plaats naar het gebruik van datamining als opsporingsmiddel. Daarbij worden de volgende uitgangspunten gehanteerd:
- onderzoek naar en verwerken van gegevens is slechts toelaatbaar bij een verdenking of een verkennend onderzoek, danwel in verband met een onderzoek naar georganiseerde criminaliteit zonder dat er sprake is van een concrete verdenking;
- het verwerken van gegevens en de daarbij te gebruiken technieken kunnen een forse inbreuk op het recht op privacy opleveren. De afweging tussen tussen het opsporingsbelang en het belang van de privacybescherming dient daarom nauwkeurig plaats te vinden. Zo dient bijvoorbeeld telkens duidelijk te worden gemaakt in de wet of het gaat om incidentele bevragingen op persoon of dat ook datamining en soortgelijke technieken mogelijk is.

Beoogd resultaat:	onderzoeksresultaat als basis voor beleid terzake strafrechtelijke handhaving.
Omschrijving activ.:	uitvoering onderzoek.
Samenhang:	gewenst evenwicht tussen belang privacy en belang strafrechtelijke rechts handhaving/hangt samen met o.a. 6 (deels).
Prioriteit:	middel, aanvang werkzaamheden 2e helft 1998, streefdatum eindresultaat 1e helft 1999. Daarna eventueel vervolg in de vorm van monitoring.
Verantwoordelijk:	Ministerie van Justitie.

2. Onderzoek vindt plaats naar de aard, ernst en omvang van ICT-criminaliteit en gebruik van opsporingsbevoegdheden in dit verband.

Beoogd resultaat:	onderzoeksresultaat als basis voor beleid terzake strafrechtelijke handhaving.
Omschrijving activ.:	uitvoering onderzoek.
Samenhang:	beter inzicht in ernst en omvang problematiek.
Prioriteit:	hoog, aanvang werkzaamheden 1e helft 1998, streefdatum eindresultaat 1e helft 1999.
Verantwoordelijk:	Ministerie van Justitie.

3. De Tweede Kamer zal nader worden geïnformeerd over de voornemens op het gebied van organisatie, opleiding en uitrusting van politie- en justitiefunctionarissen met het oog op een goede strafrechtelijke rechtshandhaving op de elektronische snelweg.

Beoogd resultaat:	beleidsnota naar Tweede Kamer.
Omschrijving activ.:	voorbereiden beleidsnota i.o.m. politie en justitie.
Samenhang:	invulling belang strafrechtelijke rechtshandhaving.
Prioriteit:	juni 1998.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Binnenlandse Zaken.

4. Het kabinet zal de oprichting van een centraal informatiepunt voor het verkrijgen van abonneegegevens ten behoeve van het bevoegd tappen bevorderen en daartoe regelgeving voorbereiden.

Beoogd resultaat:	blauwdruk voor oprichting informatiepunt; indiening wetsvoorstel.
Omschrijving activ.:	Fase 1: inventarisatie van lopende activiteiten, opstellen werkplan, dat in ieder ingaat op de organisatie en de benodigde regelgeving; Fase 2: uitvoering werkplan.
Samenhang:	strafrechtelijke rechtshandhaving moet ook in geliberaliseerde telecom-omgeving mogelijk blijven/ hangt samen met 2.3.
Prioriteit:	hoog, Fase 1: aanvang werkzaamheden 1e helft 1998; werkplan gereed 2e helft 1998; Fase 2: aanvang 2e helft 1998; afronding 2e helft 1999.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Binnenlandse Zaken, Ministerie van Verkeer en Waterstaat.

5. Het kabinet zal het initiatief nemen om binnen OESO-verband een studie te laten verrichten naar de lokalisatie van elektronische transacties en de werkelijke leiding van rechtspersonen.

Beoogd resultaat:	onderzoeksresultaat als basis voor beleid terzake strafrechtelijke handhaving (en evt. wettelijke maatregelen).
Omschrijving activ.:	Fase 1: initiëren onderzoek bij OESO; Fase 2: begeleiding uitvoering onderzoek.
Samenhang:	beter inzicht in ernst en omvang problematiek/ samenhang met 12.
Prioriteit:	aanvang Fase 1: 1e helft 1998; streefdatum afronding fase 1: 1e helft 1999.
Verantwoordelijk:	Ministerie van Justitie.

4. Bestuursrecht

1. In de Algemene wet bestuursrecht wordt een experimenteerbepaling opgenomen, waarin elektronische documenten onder voorwaarden gelijk kunnen worden gesteld aan schriftelijke documenten.

Beoogd resultaat:	indiening wetsvoorstel.
Omschrijving activ.:	normaal wetgevingsproces, aan te vangen met adviesaanvraag aan Cie Scheltema.
Samenhang:	faciliteren betrouwbaar elektronisch rechtsverkeer/ vormt basis voor structurele regeling.
Prioriteit:	hoog, adviesaanvraag 1e helft 1998; streefdatum indiening: 1e helft 1999.
Verantwoordelijk:	Ministerie van Justitie.

5. Communicatie met de overheid

1. Het kabinet zal maatregelen nemen ter bevordering van de elektronische ontsluiting van openbare registers. Het gaat hierbij in ieder geval om:

- Het elektronisch ontsluiten van bestaande curatelen- en handelsregisters en de voorbereiding van daartoe noodzakelijke regelgeving.
- Nader onderzoek naar de vraag of en, zo ja, hoe (onderdelen van) openbare registers elektronisch toegankelijk kunnen worden gemaakt voor de uitvoering van wettelijke verplichtingen, zoals bijvoorbeeld het verbod bepaalde transacties aan te gaan met minderjarigen. Bij dit onderzoek wordt de behoefte aan internationale afspraken in verband met grensoverschrijdende verificatiebehoeften betrokken.
- Het inrichten van elektronisch toegankelijke verificatieregisters waarmee organisaties die onderworpen zijn aan een identificatieplicht of die anderszins een maatschappelijk erkend belang nastreven, op een passende manier de geldigheid van een identificatiebewijs kunnen (laten) controleren.
- Bevorderen van samenwerking en kennisbundeling met betrekking tot binnen- en buitenlandse identiteitsbewijzen en achterliggende brondocumenten.
- Initiatieven om tot een elektronische ontsluiting te komen van de handelsregisters in EU-verband.

Beoogd resultaat:	Nader plan van aanpak voor ontsluiten registers; indiening wetsvoorstel; aanvang onderhandelingen in EU-verband.
Omschrijving activ.:	Fase 1: inventarisatie van lopende activiteiten, opstellen werkplan, dat in ieder ingaat op de organisatie en de benodigde regelgeving; Fase 2: uitvoering werkplan; betrekken van de Registratiekamer.
Samenhang:	faciliteren elektronisch rechtsverkeer.
Prioriteit:	middel, Fase 1: aanvang werkzaamheden 2e helft 1998, afronding eind 1998; Fase 2: aanvang werkzaamheden 1e helft 1999, afronding 2e helft 1999.
Verantwoordelijk:	Ministerie van Binnenlandse Zaken, Ministerie van Justitie, Ministerie van Economische Zaken, minister van Verkeer en Waterstaat.

2. Het kabinet zal bevorderen dat zelfregulering tot stand komt omtrent de duurzaamheid van belangrijke documenten in het maatschappelijk verkeer (I).
Tevens vindt een inventarisatie plaats van de wettelijke bepalingen waarin duurzaamheidseisen worden gesteld aan het bewaren van in het maatschappelijk verkeer belangrijke (elektronische) documenten, zoals authentieke akten met het oog op de vaststelling of technologie-afhankelijke normen nodig zijn, wat de doelstelling van de bewaring is en wat daarom de vereiste tijdsduur van de bewaring moet zijn (II).

Beoogd resultaat:	totstandkomen zelfregulering die aan waarborgen toetsingskader voldoet (I), onderzoeksresultaat als basis voor besluitvorming over evt. wetgeving (II).
Omschrijving activ.:	initiëren overleg met branche-organisaties, uitvoeren onderzoek.
Samenhang:	faciliteren betrouwbaar elektronisch rechtsverkeer.
Prioriteit:	middel, aanvang werkzaamheden 2e helft 1998; streefdatum eindresultaat 1e helft 1999.
Verantwoordelijk:	Ministerie van Binnenlandse Zaken, Ministerie van Justitie.

6. Privacy

1. Het kabinet zal, in aanvulling op de Wet bescherming persoonsgegevens, maatregelen nemen ter bevordering van de privacy. Het gaat hierbij in ieder geval om:

- Bevorderen van de oprichting – door middel van zelfregulering door diverse branches – van een aanspreekpunt voor burgers die niet willen worden gestoord in verband met commerciële aanbiedingen (het zogenaamde opt-out recht). Het initiatief van de direct-marketing branche kan hierbij als voorbeeld dienen (I).
- Voorlichting geven over aan geregistreerde toegekende rechten en over verplichtingen van verantwoordelijken ten aanzien van geregistreerde, alsmede over de mogelijkheden zelf persoonsgegevens af te schermen met behulp van beveiligingstechnieken (II).
- Bevorderen, in nauw overleg met de Registratiekamer, dat zoveel mogelijk organisaties privacyfunctionarissen benoemen, die de hun in de Wet bescherming persoonsgegevens toegekende taak zullen uitvoeren en tevens zullen fungeren als aanspreekpunt voor burgers (III).
- Bevorderen van het gebruik van PET en anonieme biometrie, in het bijzonder binnen de overheid. Hierbij geldt als restrictie dat indien hogere belangen (o.a. staatsveiligheid en voorkoming, opsporing en vervolging van strafbare feiten) dat vergen, de gegevens (terug) te herleiden moeten zijn naar concrete personen (IV).

Beoogd resultaat:	totstandkomen aanspreekpunt (I), totstandbrengen voorlichting (II), benoeming privacyfunctionarissen (III), veelvuldig gebruik van PET en anonieme biometrie.
Omschrijving activ.:	Fase 1: inventarisatie van lopende activiteiten, opstellen werkplan, dat in ieder ingaat op de organisatie; Fase 2: uitvoering werkplan.
Samenhang:	facilitering van de uitoefening van toegekende rechten door burgers.
Prioriteit:	middel, Fase 1:aanvang werkzaamheden 2e helft 1998; streefdatum eindresultaat: 1e helft 1999; fase 2: aanvang 1e helft 1999; streefdatum eindresultaat eind 1999.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Binnenlandse Zaken.

2. Het kabinet zal streven naar verdergaande internationale harmonisatie van privacynormen, in aanvulling op de EU-privacyrichtlijnen. Het gaat hierbij om:

- Bevorderen van de invulling van de in OESO-verband ontwikkelde «Guidelines on the protection of privacy and transborder flows of personal data».
- Indien blijkt dat de invulling van de normen voor gegevensbescherming op belangrijke terreinen (bijvoorbeeld verzekerings- en bankwezen) binnen de lidstaten van de EU te ver uit elkaar loopt, bevorderen van de sectorale invulling van deze normen.

Beoogd resultaat:	aanvang internationale onderhandelingen over verdergaande harmonisatie.
Omschrijving activ.:	initiëren internationaal overleg in verband van OESO en EU; bevorderen inventarisatie door Eur. Cie.
Samenhang:	verbeterde privacybescherming in internationale omgeving; ondersteunt meersporenaanpak internationalisering en rechtsmacht (zie 12).

Prioriteit:	laag, afhankelijk van inwerkingtreding Wet bescherming persoonsgegevens.
Verantwoordelijk:	Ministerie van Justitie.

7. Vrijheid van meningsuiting

1. Artikel 7 van de Grondwet wordt aangepast.

Beoogd resultaat:	indiening wetsvoorstel en daaraan voorafgaand: nader onderbouwend onderzoek.
Omschrijving activ.:	proces Grondwetswijziging.
Samenhang:	toesnijden tekst op nieuwe technologieën.
Prioriteit:	laag, hangt samen met parlementaire behandeling in twee lezingen.
Verantwoordelijk:	Ministerie van Binnenlandse Zaken, Ministerie van OCW.

2. Het kabinet zal bevorderen dat maatregelen worden genomen ter bescherming van minderjarigen tegen schadelijke informatie. Het gaat hierbij om:
- Bevorderen dat door middel van zelfregulering een classificatiesysteem voor mediaproducten tot stand komt.
- Vervolg geven aan Europees onderzoek naar mogelijkheden ter bevordering van de controle door ouders op kijkgedrag van minderjarigen.

Beoogd resultaat:	totstandkomen zelfregulering die aan waarborgen toetsingskader voldoet, onderzoeksresultaat ter onderbouwing besluitvorming.
Omschrijving activ.:	initiëren overleg met brancheorganisaties; initiëren onderzoek bij EU.
Samenhang:	bescherming van jeugdige tegen schadelijke invloeden van audiovisuele media.
Prioriteit:	hoog, aanvang werkzaamheden 1e helft 1998; streefdatum. eindresultaat: 2e helft 1998.
Verantwoordelijk:	Ministerie van VWS, Ministerie van OCW, Ministerie van Justitie.

8. Biometrie en identificatie

1. Met het oog op het bevorderen van het gebruik van biometrie zal:
- Een algemene wettelijke basis voor het gebruik van biometrie voor de uitvoering van publieke taken worden gecreëerd (fase I).
- Het kabinet stappen ondernemen om in EU-verband te komen tot een nadere wettelijke regeling voor de opslag en het gebruik van gepersonaliseerde biometrische gegevens (fase II).
- Het kabinet bevorderen dat omtrent het gebruik van biometrische technieken en databanken met biometrische persoonskenmerken internationale afspraken tot stand komen. Voor zover het daarbij gaat om standaardisatie kan met vormen van zelfregulering worden volstaan (fase II).
- Er moet worden onderzocht of een bagatel-regeling nodig is voor kleinschalig gebruik van biometrische persoonsgegevens die qua aard moeten worden gezien als «gevoelig» in de zin van de Wbp, maar in de praktijk reeds zijn ingeburgerd.

Beoogd resultaat:	indiening wetsvoorstel, bevorderen van het gebruik van biometrische legitimatie bewijzen, internationale harmonisatie van het gebruik van biometrische persoonsgegevens, onderzoeksresultaat.
Omschrijving activ:	normaal wetgevingsproces, overleg voeren met lagere overheden over het gebruik van biometrische legitimatiebewijzen, initiëren van wettelijke regelingen in EU-verband en het nemen van initiatief tot het maken van internationale afspraken over het gebruik van biometrische gegevens.
Samenhang:	bevorderen van de betrouwbaarheid van het elektronisch rechtsverkeer en verbeterde privacybescherming.
Prioriteit:	hoog: fase I, aanvang werkzaamheden 1e helft 1998, laag: fase II, aanvang werkzaamheden 1e helft 1999.
Verantwoordelijk:	Ministerie van Binnenlandse Zaken, Ministerie van Justitie.

2. Het kabinet zal ter bevordering van elektronische identificatie:
- Het personaliseren van chipkaarten en andere elektronische identiteitsbewijzen die een strikt persoonlijk toegang geven tot de elektronische snelweg onder de werking van de Wet op de identificatieplicht brengen. Tevens worden achterliggende specifieke wetten uitgebreid. Voor kleinschalige elektronische toepassingen wordt met een bagatel-regeling volstaan (fase I).
- Onderzoek laten plaatsvinden naar de ontwikkeling van elektronische equivalenten voor de schriftelijke en bij de wet erkende, identificatiedocumenten (fase I).

Beoogd resultaat:	indiening wetsvoorstel, uitvoering geven aan de Wet op de identificatieplicht, inzicht krijgen in de technische mogelijkheden ten behoeve van elektronische identificatie.
Omschrijving activ.:	normaal wetgevingsproces, uitvoeren van onderzoek.
Samenhang:	bevorderen van de betrouwbaarheid van elektronisch rechtsverkeer.
Prioriteit:	hoog: fase I, aanvang werkzaamheden 1e helft 1998, indiening wetsvoorstel 1e helft 1999, afronding onderzoek 2e helft 1998, laag: fase II, is afhankelijk van fase I.
Verantwoordelijk:	Ministerie van Binnenlandse Zaken, Ministerie van Justitie.

3. Er wordt regelgeving voorbereid voor de digitale handtekening, waarbij wordt aangesloten bij een binnenkort te verwachten voorstel voor EU-regelgeving.

Beoogd resultaat:	indiening wetsvoorstel.
Omschrijving activ.:	normaal wetgevingsproces.
Samenhang:	bevorderen van de betrouwbaarheid van elektronisch rechtsverkeer en privaatrechtelijke rechtshandhaving.
Prioriteit:	middel, afhankelijk van voorbereiding EU-richtlijn.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Economische Zaken, Ministerie van Verkeer en Waterstaat, Ministerie van Binnenlandse Zaken.

9. Trusted Third Parties

1. Het kabinet zal de totstandkoming van Trusted Third Parties met faciliterende wetgeving ondersteunen, ten minste door het verlenen van bewijskracht in het Wetboek van Burgerlijke Rechtsvordering aan door bepaalde TTPs vastgelegde elektronische informatie;

Beoogd resultaat:	indiening wetsvoorstel.
Omschrijving activ.:	normaal wetgevingsproces.
Samenhang:	bepalend voor implementatie nota/bevorderen van de betrouwbaarheid van het elektronisch rechtsverkeer, ondersteunen van het bewijsrecht, belang van de strafrechtelijke rechtshandhaving.
Prioriteit:	hoog, aanvang werkzaamheden 1e helft 1998, streefdatum indiening 1e helft 1999/hangt samen met notitie van Verkeer en Waterstaat en Economische Zaken over TTP's.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Economische Zaken, Ministerie van Verkeer en Waterstaat, Ministerie van Binnenlandse Zaken.

2. Het kabinet zal bevorderen dat zelfregulering tot stand komt voor TTP's, voortbouwend op ervaringen die zijn opgedaan bij andere intermediaire instanties, zoals de accountancy en het notariaat, zulks ter uitvoering van de notitie over TTP's, die de Ministers van Verkeer en Waterstaat en EZ in voorbereiding hebben.

Beoogd resultaat:	goed stelsel van TTP's en eventueel faciliterende regelgeving.
Omschrijving activ.:	overleg voeren met de branche-organisaties en ondersteuning verlenen bij het opstellen van regelgeving, alsmede eventueel voorzien in een stelsel van toezicht.
Samenhang:	bevorderen van de betrouwbaarheid van het elektronisch rechtsverkeer.
Prioriteit:	vloeit voort uit de notitie van het Ministerie van Verkeer en Waterstaat en Ministerie van Economische Zaken.
Verantwoordelijk:	Ministerie van Economische Zaken, Ministerie van Verkeer en Waterstaat, Ministerie van Justitie, Ministerie van Binnenlandse Zaken.

10. Marktwerking

1. Onderzoek naar de mogelijkheid van dwanglicenties, waar standaardisatie verhinderd wordt door misbruik van octrooirecht.

Beoogd resultaat:	onderzoek van de geschiktheid van dwanglicenties voor de opening van standaarden.
Omschrijving activ.:	verrichten van onderzoek.
Samenhang:	bevorderen van mededinging.
Prioriteit:	middel, aanvang onderzoek 2e helft 1998.
Verantwoordelijk:	Ministerie van Economische Zaken en Ministerie van Justitie.

2. Onderzocht wordt of het zinvol is het regime van de Telecommunicatiewet op het gebied van interconnectie ook toe te passen op andere informatiemarkten.

Beoogd resultaat:	onderzoek of het wenselijk en noodzakelijk is interconnectie verplichtingen op te leggen.
Omschrijving activ.:	verrichten van onderzoek.
Samenhang:	bevorderen van mededinging.
Prioriteit:	laag, aanvang onderzoek 1e helft 1999.
Verantwoordelijk:	Ministerie van Verkeer & Waterstaat.

3. Het kabinet zal er op toezien dat het stelsel van zelfregulering voor het toewijzen van adressen en domeinnamen voldoet aan de in het toetsingskader gestelde eisen.

Beoogd resultaat:	goed stelsel van adres en domeinnaamtoewijzing.
Omschrijving activ.:	overleg voeren met de Stichting Internet Domeinregistratie Nederland.
Samenhang:	transparantie van toewijzing en eerbiediging van rechten van intellectuele eigendom.
Prioriteit:	hoog, aanvang overleg 1e helft 1998.
Verantwoordelijk:	Ministerie van Economische Zaken, Ministerie van Verkeer en Waterstaat.

4. Het kabinet zal stappen ondernemen om te komen tot nadere internationale afspraken die de samenwerking tussen mededingingsautoriteiten bevorderen. Deze stappen worden op EU-niveau ingezet.

Beoogd resultaat:	verkrijgen van positieve samenwerking tussen mededingingsautoriteiten (possitive commity).
Omschrijving activ.:	initiëren van overleg hierover in de Europese commissie, waarbij de mededingingsautoriteiten moeten worden betrokken.
Samenhang:	kunnen optreden tegen overtreding van het (Nederlandse) mededingingsrecht.
Prioriteit:	middel, aanvang overleg 2e helft 1998.
Verantwoordelijk:	Ministerie van Economische Zaken.

5. Het kabinet zal de uitbreiding van standaardisatie van technische normen en koppelvlakken bevorderen, bij voorkeur via internationale standaardorganisaties.

Beoogd resultaat:	standaardisatie.
Omschrijving activ.:	initiëren van overleg met internationale standaardorganisaties.
Samenhang:	bevorderen mededinging.
Prioriteit:	hoog, aanvang werkzaamheden 1e helft 1998.
Verantwoordelijk:	Ministerie van Economische Zaken, Ministerie van Verkeer en Waterstaat.

11. Internationalisering en rechtsmacht (nationale uitvoering)

In bestuursrechtelijke vergunningenstelsels worden voorzieningen opgenomen, die moeten voorkomen dat buitenlandse dienstenaanbieders het Nederlandse of Europese recht kunnen omzeilen. De wijze waarop hieraan vorm wordt gegeven, moet verenigbaar zijn met (toekomstige) regelgeving van de Europese Unie en de WTO.

Beoogd resultaat:	div. wetsvoorstellen.
Omschrijving activ.:	Fase 1: inventariserend onderzoek, waaronder toetsing bij Europese Commissie en WTO; Fase 2: normaal wetgevingsproces.
Samenhang:	creëren van een fysiek aangrijpingspunt t.b.v. de rechtsmacht van Nederland /hangt samen met 12.

Prioriteit:	middel, aanvang fase1: 2e helft 1998; aanvang fase 2: 1e helft 1999; streefdatum indiening eind 1999.
Verantwoordelijk:	Ministerie van Justitie, Ministerie van Economische Zaken.

12. internationalisering en rechtsmacht (inbreng in internationale gremia)

1. Het kabinet zal de voorstellen van de nota over internationalisering en rechtsmacht, op het gebied van het privaatrecht, inbrengen in de daartoe geëigende internationale organisaties. Het gaat hierbij in ieder geval om:
- Bevorderen van de totstandkoming van mondiale ipr-regels inzake Internet in het kader van de Haagse Conferentie.
- Bevorderen dat internationale organisaties zoals UNCITRAL, UNIDROIT en de Internationale Kamer van Koophandel internationaal privaatrechtelijke beginselen voor elektronische handel definiëren, waarbij deelnemers aan elektronische handel dienen te worden betrokken.
- Zo mogelijk mondiaal, maar in ieder geval in het kader van de Raad van Europa bevorderen:
  – de totstandkoming van een uniforme regeling voor de privaatrechtelijke aansprakelijkheid van tussenpersonen voor onrechtmatige daden;
  – de totstandkoming van een regeling over de reconstructie door de burger van een elektronisch spoor, teneinde hem in staat te stellen te achterhalen waar vandaan jegens hem een onrechtmatige daad wordt gepleegd.

Beoogd resultaat:	aanvang cq. intensivering van internationale onderhandelingen.
Omschrijving activ.:	Fase 1: opstellen werkplan; Fase 2: initiëren cq. bevorderen internationaal overleg.
Samenhang:	bepalend voor implementatie nota/nauwe samenhang met 12.2 en 12.3.
Prioriteit:	hoog, fase 1: 1e helft 1998; fase 2: afh. van werkplan.
Verantwoordelijk:	Ministerie van Justitie.

2. Het kabinet zal de voorstellen van de nota over internationalisering en rechtsmacht, op het gebied van het strafrecht, inbrengen in de daartoe geëigende internationale organisaties. Het gaat hierbij in ieder geval om:
- Bij internationale organisaties te pleiten voor internationale regelingen van de strafrechtelijke aansprakelijkheid van tussenpersonen. Hierbij kan worden gedacht aan de Raad van Europa en de OESO. Daarbij worden de oplossingen in het Wetsvoorstel Computercriminaliteit II uitgedragen.
- Bevorderen dat regels tot stand komen over samenwerking tussen opsporingsautoriteiten teneinde een effectieve handhaving te bereiken over onder meer opsporing op buitenlandse computers en medewerking van andere landen bij de opsporing.
- Overwegen af te zien van de eis van dubbele strafbaarheid bij het verlenen van rechtshulp, mits er geen sprake is van uitlevering. De rechtshulp zal enkel zien op informatieverschaffing, teneinde het elektronisch spoor te kunnen reconstrueren. Bovendien zal aan enkele voorwaarden voldaan moeten worden, zoals afspraken op basis van reciprociteit, alleen rechtshulp bij van te voren bepaalde ernstige delicten, het delict zal moeten zijn gericht op de rechtsorde van het land dat om rechtshulp verzoekt en notificatie achteraf aan de betrokken persoon.
- Bevorderen dat de werkzaamheden van het Committee of experts on crime in cyber-space (PC-CY) van de Raad van Europa worden uitgebreid. Deze groep zou zich ook moeten buigen over:

de rechtsmacht en het toepassen van bijzondere opsporingsbevoegdheden in de elektronische omgeving.
- De voorwaarden waaronder deze bijzondere opsporingsbevoegdheden in de elektronische omgeving mogen worden toegepast op het moment dat daardoor de soevereiniteit van een ander land wordt geraakt.

Beoogd resultaat:	aanvang cq. intensivering van internationale onderhandelingen.
Omschrijving activ.:	Fase 1: opstellen werkplan; Fase 2: initiëren cq. bevorderen internationaal overleg.
Samenhang:	bepalend voor implementatie nota/nauwe samenhang met 12.1 en 12.3.
Prioriteit:	hoog, fase 1: 1e helft 1998; fase 2: afh. van werkplan.
Verantwoordelijk:	Ministerie van Justitie.

3. Het kabinet zal de voorstellen van de nota over internationalisering en rechtsmacht, die rechtsgebiedoverstijgend zijn inbrengen in de daartoe geëigende internationale organisaties, aan de hand van een strategie, die in een nader werkplan wordt vastgelegd. Het gaat hierbij in ieder geval om:
- Bevorderen van internationale harmonisatie van materiële normen waar dat kansrijk is, zoals in het privaatrecht, bij economische ordeningswetgeving, vermogensdelicten, specifieke computerdelicten en vergrijpen waarover een brede internationale consensus bestaat (kinderporno en extreem geweld).
- Het ontstaan van vrijhavens trachten te beperken door internationale afspraken te maken over de mogelijkheden voor het opleggen van economische sancties.
- Bevorderen van de totstandkoming van internationale regels over het uitoefenen van rechtsmacht. Indien dit niet haalbaar is, moeten er afspraken worden gemaakt over onderlinge prioritering bij de uitoefening van rechtsmacht, waarbij naar analogie van de aanknopingsleer van het IPR een oplossing kan worden gezocht.
- De internationale gedachtenvorming bevorderen over een specifiek verdrag voor Internet.
- Bevorderen dat internationale zelfregulering tot stand komt voor de belangrijkste actoren op het gebied van de elektronische snelweg als alternatief voor (inter)nationale regelgeving. Daarbij moet worden gekeken naar de mogelijkheden voor een publiekrechtelijk toezicht op die zelfregulering, waarmee een sluitend en handhaafbaar regime mogelijk wordt dat bovendien kwetsbare belangen in voldoende mate beschermt.

Beoogd resultaat:	Fase I: Werkplan, dat in ieder geval ingaat op de prioriteitsvolgorde van de verschillende onderdelen, de vraag waar Nederland initiatief moet nemen en waar zij kan afwachten, de meest geschikte internationale organisatie per onderwerp, Fase II: uitvoeren werkplan.
Omschrijving activ.:	Fase I: Opstellen werkplan en toetsen werkplan bij int. organisaties; Fase II: hangt af van werkplan.
Samenhang:	bepalend voor implementatie nota/nauwe samenhang met 12.1 en 12.2.
Prioriteit:	hoog, fase 1: 1e helft 1998; fase 2: afh. van werkplan.
Verantwoordelijk:	Ministerie van Justitie.

13. Toegevoegd project: actualisering nota

Twee jaar na het verschijnen van de Kabinetsnota vindt een actualisering plaats, waarbij wordt bezien of toekomstige gesignaleerde knelpunten zich ook daadwerkelijk voordoen. Bij de actualisering worden in ieder geval onderwerpen bezien, waarin rol van de wetgever afhangt van:

- De technologische ontwikkelingen of,
- Hoe de verhouding tussen nieuwe en traditionele media zich ontwikkelt.

Beoogd resultaat:	actualiserende notitie t.b.v. Tweede Kamer.
Omschrijving activ.:	Voorbereiding notitie.
Samenhang:	n.v.t.
Prioriteit:	aanvang werkzaamheden eind 1999; afronding: april 2000.
Verantwoordelijk:	Ministerie van Justitie, zo mogelijk binnen het kader van het tweede Nationaal Actieprogramma Elektronische snelwegen.

Toelichting: in ieder geval komen de volgende onderwerpen aan de orde in de actualisering:

- Aanpassing van de regelgeving op het punt van de bescherming tegen inbreuken door technische oorzaken in aanvulling op de voorzieningen in de nieuwe Telecommunicatiewet en in het Burgerlijk Wetboek.
- Een eventueel verbod op het wijzigen van stromende informatie.
- Geheimhoudingsbepalingen voor beroepsgroepen die met vertrouwelijke gegevens omgaan.
- Monitoring en beoordeling van de ontwikkelingen en van de effectiviteit van de activiteiten van de NMA en OPTA, met in achtneming van de conclusies en voorstellen van het MDW-rapport «Zicht op toezicht».
- Toepassing van het regime voor de universele dienstverlening van de Telecommunicatiewet in de sfeer van Internet.
- Regels inzake de toegang tot Internet voor zover overheden exclusief of in belangrijke mate informatie gaan aanbieden via Internet, danwel de communicatie met overheidsfunctionarissen exclusief of in belangrijke mate via Internet moet plaatsvinden.
- Regels inzake de toegang tot Internet in meer algemene zin.
- Toepassen van het stimuleringsregime dat thans bestaat voor de traditionele media (bedrijfsfonds voor de pers, publieke radio- en tv-producties) op de elektronische snelweg.
- Regelgeving over informatiemonopolies.
- Algemene regels met betrekking tot middelen tot bewaring van rechten in het bijzonder beslag op gegevensbestanden, in het Wetboek van Burgerlijke Rechtsvordering.
- Invulling van de wettelijke eisen met betrekking tot tappen, teneinde discriminatie van telecommunicatie-aanbieders te voorkomen.
- De hanteerbaarheid van in de Telecommunicatiewet gemaakte technische onderscheidingen waaraan verschillende rechtsplichten en/of -gevolgen worden verbonden.

DEEL VI BIJLAGEN

Bijlage 1

Overzicht geraadpleegde literatuur

Aanwijzingen voor de regelgeving, aanwijzingen voor convenanten: praktijkvoorschriften voor ontwerpers van regelingen en convenanten van de rijksoverheid / Ministerie van Justitie. – Den Haag, 1996. – (Gereedschap voor de wetgevingspraktijk; 4)

Actieprogramma Elektronische Snelwegen: «van metafoor naar actie»

Amongst friends in computers and law / H.W.K. Kaspersen (ed.) and A. Oskamp (ed.). – Deventer, 1990. – (Computer law series; 8)

Andeweg, R.B. / Overheid of overhead: de bestuurbaarheid van het overheidsapparaat, in: Het schip van staat. – Zwolle, 1985

Andriessen, J.E. en R.F. van Esch / Globalisering: een zekere trend. – Den Haag: Ministerie van Economische Zaken, 1993. – (Discussienota; 9301)

Arnbak, J.C., J.J. van Cuilenburg en E.J. Dommering / Verbinding en ontvlechting in de communicatie: een studie naar toekomstig overheidsbeleid voor de openbare elektronische informatievoorziening. – Amsterdam, 1990

Backx, H.A.M. / Normalisatie en certificering als alternatieven voor en in wettelijke regelingen. – RegelMaat 1995, afl. 3, p. 89–100

Beukel, J. van den / Toegang tot de televisiemarkt. – Deventer, 1995

Beunen, Annemarie / Digitale manipulatie van beeldmateriaal. – Alphen aan den Rijn, 1997. – (ITeR; 6)

Brandeis, L., and Warren / The right to privacy. – Harvard law review, 15 december 1890
De digitale handtekening: juridische en organisatorische aspecten / ITeR workshop van 17 december 1996. – Alphen aan den Rijn, 1997

Compendium van het staatsrecht / Th.L. Bellekom ... [et al.] (bew.). – Deventer, 1994

Consumentenrecht op de elektronische snelweg: themanummer. – Tijdschrift voor consumentenrecht, 1997, afl. 3

Convenanten tussen overheid en maatschappelijke organisaties / F.J. van Ommeren en H.J. de Ru. – 's-Gravenhage, 1993

Craats, J. van de / Pasjes en pincodes: over de cryptologie van plastic geld. – Bloemendaal, 1991

Derksen, W. / De werkelijkheid van de terugtred, in: De terugtred van regelgevers. – Zwolle, 1989

Diensten en infrastructuren voor Elektronische Snelwegen in Nederland: rapport in opdracht van de Initiatiefgroep Infrastructuur Elektronische Snelwegen en de Kerngroep Diensten Elektronische Snelwegen / M&I/Partners. – Amersfoort, 1996

Donner, J.P.H. / Notitie informatie en telecommunicatie: publiek domein. – Den Haag: WRR, 1996

Donner, J.P.H. / De relativiteit van zelfregulering, in: Overheid en zelfregulering. – Zwolle, 1993

Dorbeck-Jung, B.R. / Rechtsstaat en zelfregulering, in: Tussen overheid en samenleving. – Enschede, 1992

Dorbeck-Jung, B.R. / Wettelijk geconditioneerde zelfregulering: symbolisch concept of instrument met gevolgen?, in: Overheid en zelfregulering. – Zwolle, 1993

Draaiboek voor de wetgeving: systematische beschrijving van de procedure / Ministerie van Justitie. – Den Haag, 1996. – (Gereedschap voor de wetgevingspraktijk)

Eijlander, Ph. / Zelfregulering en wetgevingsbeleid, in: Overheid en zelfregulering. – Zwolle, 1993

Emerging electronic highways / Victor Bekkers, Bert Jaap Koops and Sjaak Nouwt (ed.). – Den Haag, 1996

Engbersen, Godfried / Publieke bijstandsgeheimen: het ontstaan van een onderklasse in Nederland. – Leiden, 1990

Esch, R.E. van en R.E. de Rooy / Juridische aspecten van Internetbetalingen. – Nederlands Juristenblad 1996, afl. 41

Evaluatie Internet meldpunt kinderporno / Felipe Rodriquez-Svensson en Christine Karman (red.). – Amsterdam, 1997

Frissen, P.H.A. / De virtuele staat: politiek, bestuur, technologie: een postmodern verhaal. – Schoonhoven, 1996

Frissen, P.H.A. / Zelfregulering en besturingsconcepties, in: Overheid en zelfregulering. – Zwolle, 1993

Gardeniers, H.J.M. / Chipcards en privacy: regels voor een nieuw kaartspel. – Rijswijk: Registratiekamer, 1995

Geelhoed, L.A. / Deregulering, herregulering en zelfregulering, in: Overheid en zelfregulering. – Zwolle, 1993

Geelhoed, L.A. / Plaats en toekomst van de wetgever in een informatiemaatschappij, in: De overheid op weg naar de informatiemaatschappij. – Leiden, 1988

Geelhoed, L.A. en R.J. in 't Veld / Vervlechting en verschuivingen in wetgevingscomplexen aan het begin van de 21ste eeuw. – Zwolle, 1996. – (Publikaties van de Staatsrechtkring; 12)

Grijpink, Jan / Keteninformatisering. – Den Haag, 1997

Een haalbare «card»: consequenties voor opsporing en vervolging / A. Knopjes en P.J. Lakeman (red.). – Zoetermeer, 1996. – (CRI themaboek)

Handboek van het Nederlandse staatsrecht / Van der Pot, Donner. – Zwolle, 1995

Handelen met de sterke arm, deel II ; rapport institutioneel onderzoek naar het beleidsterrein «politie» 1994 / M.J.B. Kavelaars (samenst.). – Den Haag, 1996. – (PIVOT-rapporten)

Handelend optreden: overheidshandelen: modellen, onderzoeksmethoden en toepassingen / PIVOT. – 's-Gravenhage, 1994. – (PIVOT-rapporten)

Hins, Wouter / De eeuwigdurende telecommunicatiediensten. – Alphen aan den Rijn, 1996. – (ITeR; 4)

Hins, Wouter en Bernt Hugenholtz / The law of international telecommunications in the Netherlands. – Baden-Baden, 1988. – (Law and economics of international telecommunications; 6)

Hoefnagel, F.J.P.M. / Wetgever en cultuur. – Zwolle, 1988

Hof, Simone van der / De juridische status van de digitale handtekening. – Alphen aan den Rijn, 1997. – (ITeR; 7)

Hof, Simone van der / Overheidsinformatie in de etalage. – Alphen aan den Rijn, 1997. – (ITeR; 5)

Hofman, J.A. / Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht. – Zwolle, 1995

Holvast, Jan / Persoonsgegevens of niet: dat is de vraag. – Alphen aan den Rijn, 1996. – (ITeR; 2)

Hood, Christopher C. / The tools of government. – London, 1983

Hoven van Genderen, R. van den, J. Nouwt en J.E.J. Prins / Recht op de elektronische snelweg?!: drie thema's inzake overheidsbeleid en nieuwe mogelijkheden voor informatievoorziening. – Alphen aan den Rijn, 1995. – (Preadvies ten behoeve van de Vereniging voor Informatietechnologie en Recht)

Huydecoper, Sylvia en Rob van Esch / Geschriften en handtekeningen: een achterhaald concept?. – Alphen aan den Rijn, 1997. – (ITeR; 7)

In beeld gebracht: privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging / Registratiekamer. – Den Haag, 1997

In het licht van de Wet persoonsregistraties: zon, maan of ster? / J.E.J. Prins ¼ [et al.]. – Alphen aan den Rijn, 1995. – (ITeR; 1)

De informatiemaatschappij: de gevolgen van de micro-elektronische revolutie. – Maastricht, 1983

Informatietechnologie en recht: rapport van de tijdelijke adviescommissie Informatietechnologie en Recht met betrekking tot de opzet van onderzoek op het gebied van informatietechnologie en recht / (Voorz. H. Franken). – Lelystad, 1991

Informatietechnologie en recht in Nederland: onderzoek en onderzoeksgroepen / A.H.J. Schmidt (red.). – Lelystad, 1994

Informatisering en de kwaliteit van bestuur en samenleving / T. Huppes (red.). – Deventer, 1992

Informatisering in het openbaar bestuur: technologie en sturing bestuurskundig beschouwd / A. Zuurmond ... [et al.] (red.). – 's-Gravenhage, 1994

Jong, Jitske de, Marcel Rietdijk en Yvette Pluijmers / Vastgoed persoonlijk benaderd: bescherming van persoonsgegevens binnen vastgoed-registraties. – Alphen aan den Rijn, 1997. – (ITeR; 5)

Kabinet-Kok: keuzen voor de toekomst. – Den Haag, 1994. – Bevat regeerakkoord

Kansspelen herijkt / Hans Moerland en Arjan van 't Veer (red.). – Deventer, 1996. – (Monografieën kansspelen; 3)

Kaspersen, H.W.K. / Recht en informatietechnologie: een zaak van intensief onderhoud. – Deventer, 1996

Kemna, Anne-Marie en Astrid Tuinder / Regulering van encryptie. – Alphen aan den Rijn, 1996. – (ITeR; 3)

Kleve, P. / Rechtsvragen over informatietechnologie. – Lelystad, 1996

Knobbout-Bethlem, Ch.E. / Konsumentengericht elektronisch betalings-verkeer. – Deventer, 1992. – (Consument en recht; 10)

Koers, A.W. / Rechten en plichten van het individu op de elektronische snelweg: aanzet tot een handvest. – Amsterdam , 1995. – (Fatima reeks)

Kralingen, Robert van, Corien Prins en Jan Grijpink / Het lichaam als sleutel. – Alphen aan den Rijn, 1997. – (ITeR; 8)

Krugman, P. / Peddling prosperity. – New York, 1994

Kuile, B.H. ter / Ons nationaal omroepbestel in de greep van Gemeenschapsrecht?. – Arnhem, 1995. – (SI-EUR-reeks; 7A)

Een kwestie van toegang: bijdragen aan het debat over het publieke domein van de informatievoorziening / Inigo Baten en Jolien Ubacht (samenst.). – Amsterdam, 1995. – (Fatima reeks)

Licensing of Trusted Third Parties for the provision of encryption services: public consultation paper / Department of Trade and Industry. – London, 1997

Lips, Miriam en Paul Frissen / Wiring government. – Alphen aan den Rijn, 1997. – (ITeR; 8)

Lisser, E.Ch. / Alternatieven voor wetgeving op decentraal niveau. – RegelMaat 1995, afl. 1, p. 19–31

Lyotard, J.-F. / Het postmoderne weten: een verslag. – Kampen, 1987

Massamedia en staatsrecht: de staatsrechtelijke grondslagen van het mediarecht / E.M.H. Hirsch Ballin ... [et al.] (red.). – Zwolle, 1989. – (Staatsrechtconferentie 1988)

Meningen over afluisteren / Peter J. van Koppen ... [et al.]. – Leiden: NSCR, 1993. – (Report NSCR; 93–03)

Ohmae, Kenichi / The end of the nation state. – London, 1995

Omroep en commercie 1995: adviezen, beschikkingen, uitspraken, beleidslijnen en wetgeving / Marcel Dellebeke en Jan J.C. Kabel. – Amsterdam, 1996

Op weg naar ¼ digitaal rechercheren: de invloed op en de gevolgen van de vergaande digitalisering van de Nederlandse maatschappij op het werk van politie en justitie / Beleidsadviesgroep Computercriminaliteit, 1996

Overheid en zelfregulering / Eijlander, Ph., P.C.Gilhuis en J.A.F. Peters (red.). – Zwolle, 1993

De overheid op weg naar de informatiemaatschappij: automatisering, debureaucratisering en verbeterde dienstverlening / T. Huppes (red.). – Leiden, 1988

Patijn, Alexander / Grondrechten en nieuwe communicatietechnologieën: de rol van de wetgever. – NJCM-Bulletin 1996, p. 796–806

Pessemier, Tobias de / Vrijheid van expressie en informatie op het Internet. – Gent, 1997

Plan van aanpak Elektronische Snelwegen: visie op versnellen / project-groep Elektronische Snelweg, (voorz. W.E. Scherpenhuijsen) in opdracht van stuurgroep Elektronische Snelwegen. – Den Haag, 1996

Porter, Michael E. / The competetive advantage of nations. – New York, 1990

Privacy: een kind van vele ouders:schetsen over privacy in de moderne gezondheidszorg / J.M.A. Berkvens ¼ [et al.]. – Oss, 1997

Privacy disputed / Pieter Ippel, Guus de Heij and Bart Crouwers (ed.). – Den Haag, 1995

Privacy en persoonsregistratie: eindrapport van de Staatscommissie Privacy en persoonsregistratie / (voorz. T. Koopmans). – Den Haag, 1976

Privacy in het informatietijdperk / Sjaak Nouwt en Wim Voermans (red.). – Den Haag, 1996. – (Recht, bestuur en informatisering; 2)

Privacy-enhancing technologies: the path to anonymity / Registratiekamer; TNO-FEL. – Rijswijk, 1995. – (Achtergrondstudies en verkenningen; 5B)

Privacyregulering in theorie en praktijk / J.M.A. Berkvens en J.E.J. Prins (red.). – Deventer, 1994. – (Recht en praktijk)

Publieke taak, private markt: de gevolgen van privatisering voor de publieke taakstelling / G.N.H. Kemperink (red.). – Deventer, 1995

Rademaker, Jan / De digitale strafrechtspleging. – Zwolle, 1996

Rapport: diensten en infrastructuren voor Elektronische Snelwegen in Nederland / M&I Partners. – Amersfoort, 1996

Recht op de elektronische snelweg: NJB speciaal. – Nederlands Juristenblad 1996, afl. 41, p. 1695–1759

Rechtsstaat en sturing / M.A.P. Bovens, W. Derksen en W.J. Witteveen (red.). – Zwolle, 1987

Regulering van het Internet/Ingrid van den Berg, Hielke Hijmans en Aernout Schmidt (Red), – Alphen a/d Rijn/ Diegem 1997.

Reich, Robert B. / The work of nations. – London, 1993

Reijne, Z., R.F. Kouwenberg en M.P. Keizer / Tappen in Nederland. – Arnhem, 1995. – (WODC Onderzoek en beleid; 155)

Roos, Theo de, Gerard Schuijt,en Louisa Wissink / Smaad, laster, discriminatie en porno op Internet. – Alphen aan den Rijn, 1996. – (ITeR; 3)

Rose, Lance / NetLaw: your rights in the online world. – Berkeley, 1995

Ru, H.J. de / De algemene wet gaat voor de bijzondere wet. – Den Haag: CDWO SAW, 1993. – (Achtergrondstudies Algemeen Wetgevingsbeleid)

Schut, Eric en Elke Wiersema / Betrouwbaarheid van elektronische berichten in het betalingsverkeer. – Alphen aan den Rijn, 1997. – (ITeR; 7)

Schwartz, Ivo E., J,P.H. Donner en E.J. Dommering / Omroep zonder grenzen: beschouwingen over het Kabelregeling-arrest. – Amsterdam, 1988

Slabbers, Maureen en Bart Verspragen / Stemming 2: de Nederlandse technologische positie en de invloed van globalisering. – Maastricht, 1995

Slot, P.J. / Sturing en recht, in: Het schip van staat. – Zwolle, 1985

Snellen, I.Th.M. en J.T. Schokker / Wetgeving en systeemontwikkeling. – Den Haag, 1993. – (Achtergrondstudies algemeen wetgevingsbeleid)

Snoep, T.M. / Toegang tot de kijker: een kink in de kabel?: een onderzoek naar mogelijkheden voor toepassing van de WEM in de kabeldistributie-markt. – Den Haag, 1995

Stout, Helen D. / Het labyrint van de wetgeving en de alternatieve strategieën van De Ru en Sturing op maat. – RegelMaat 1994, afl. 3, p. 97–102

Terug naar het publiek / Commissie Publieke Omroep (voorz. M. Ververs). – Den Haag, 1996

De terugtred van regelgevers: meer regels, minder sturing? / W. Derksen, Th.G. Drupsteen en W.J. Witteveen (red.). – Zwolle, 1989. – (Recht, staat en sturing)

Toeval of noodzaak: geschiedenis van de overheidsbemoeienis met de informatievoorziening / A. Mol ... [et al.]. – Amsterdam, 1995. – (Fatima reeks)

Tussenrapport werkgroep Markt en Overheid / Den Haag: Ministerie van Economische Zaken, 1996

Van overheid naar markt: theorie, praktijk en analyse. – R.H. Coops ... [et al.] (red.). – Den Haag, 1995

Veeken, L.G.M. en J.A. Knigge / De EG-richtlijn «Bescherming persoons-gegevens»: knelpunten en kosten voor het bedrijfsleven. – Zoetermeer, 1994

Veld, R.J. in 't / Zelfregulering en overheidssturing, in: Overheid en zelfregulering, Zwolle, 1993

Veld, R.J. in 't, A.J.M. Verhey en H.L. Klaassen / De organisatie van het toezicht op de marktwerking in Nederland. – Den Haag: Ministerie van Economische Zaken, 1996. – (Onderzoeksreeks directie Marktwerking)

Verberne, Maartje, Nico van Eijk en Egbert Dommering / Veilen van frequenties. – Alphen aan den Rijn, 1996. – (ITeR; 4)

Vercoulen, Frank, Jan Smits en Ted Clarkson / Nederland no 1 op de elektronische snelweg!: een misplaatste grap?. – Informatie en informatiebeleid, 1997, afl. 3, p. 59–69

Verhey, L.F.M. / De EG-richtlijn bescherming persoonsgegevens: uitgangspunten en hoofdlijnen. – NJCM-bulletin 1997, afl. 3, p. 239–256

Verzelfstandiging van overheidsdiensten: congrespublikatie 1992 / W.J.M. Kickert, N.P. Mol en A. Sorber (red.). – 's-Gravenhage, 1993. – (Geschriften van de Vereniging voor Bestuurskunde; 16)

Vlaam, Heleen de, Hans de Bruijn en Ernst ten Heuvelhof / Interconnection disputes. – Alphen aan den Rijn, 1997. – (ITeR; 8)

Vriesde, R.H.P. / De steigers voorbij: jaaroverzicht 1996 Stuurgroep Informatietechnologie en Criminaliteit. – Zoetermeer, 1997

Vroom, B. de / Zelfregulering, in: De terugtred van de regelgevers. – Zwolle, 1989

Wees, J.G.L. van der en W.G. Renden / Internet voor juristen. – Deventer, 1995

Westerbrink, B.N. / Juridische aspecten van het Internet. – Amsterdam, 1996

Wetgeven en de maat van de Tijd / Ph. Eijlander ... [et al.] (red.). – Zwolle, 1994

Wierda, G.C.Th. / Een slot op de deur: randvoorwaarden voor de rechtshandhaving op het internet. – Computerrecht 1996, afl. 6, p. 233–235

Wierda, Gerben / Over de toekomst van de wetenschappelijke informatievoorziening. – Den Haag: Adviesraad voor het Wetenschaps- en Technologiebeleid, 1995. – (Achtergrondstudie; 5)

Witteveen, W.J. / Terugtred van regelgevers in wisselend perspectief, in: De terugtred van regelgevers. – Zwolle, 1989

De WPR als zon, maan of ster / Wim van der Donk ¼ [et al.]. – Alphen aan den Rijn, 1996. – (ITeR; 2)

Zicht op toezicht / MDW-werkgroep Toezicht op nutsvoorzieningen. – Den Haag, 31 november 1997

Zoontjes, P.J.J. / De queeste naar evenwicht, in: Overheid en zelfregulering. – Zwolle, 1993

Bijlage 2

Lijst met geraadpleegde personen

1. Deskundigen

Prof. dr. J.C. Arnbak
College van bestuur
Onafhankelijke Post en Telecommunicatie Autoriteit

Prof.mr. E.J. Dommering
Instituut voor Informatierecht
Faculteit Rechtsgeleerdheid
Universiteit van Amsterdam

Mr. C. Drion
Kennedy Van der Laan Advocaten
Amsterdam

Prof. mr. H. Franken
Faculteit der Rechtsgeleerdheid
Rijksuniversiteit Leiden

Prof. dr. P.H.A. Frissen
Centrum voor Recht, Bestuur en Informatisering
Katholieke Universiteit Brabant

Prof. mr. H.W.K. Kaspersen
Instituut voor Informatica en Recht
Faculteit der Rechtsgeleerdheid
Vrije Universiteit Amsterdam

Prof. dr. A.W. Koers
Centrum voor Beleid en management
Faculteit Rechtsgeleerdheid
Rijksuniversiteit Utrecht

Prof. dr. J.E.J. Prins
Centrum voor Recht, Bestuur en Informatisering
Katholieke Universiteit Brabant

Prof. Dr. J.M. Smits
Faculteit Technologiemanagement
Technische Universiteit Eindhoven

2. Leden expertisegroep bedrijfsleven

Mw. mr. E. Aberson
Consumentenbond

Mr. A. van Bellen
Nationaal coördinatie- en kenniscentrum voor Electronic data Interchange (Ediforum)

Mr. J. Bos
DSEMCO

Drs. A. Eisner
Nederlandse Vereniging van Internetoproviders (NLIP)

Mr. R.E. van Esch
RABO Bank Nederland

Mr. M.J. Frequin
Nederlands Uitgeversverbond

Mr. H. Gardeniers
FENIT

Mr. S. Katus
VNO/NCW

Mr. W. Kroeze
Ericsson Telecommunicatie

Mr. J. Levi
VECAI

Mw.mr. G.N. Sciarone
Netwerkdiensten Strategie, PTT Telecom

3. Deelnemers ITeR-workshops

Amsterdam, 26 februari , 5 en 19 maart 1997
Deelnemerslijst in Regulering van het Internet, 1997, blz. 45, 102 en 158

Bijlage 3 **Parlementaria – wetgeving**

20 644, TK 1996–1997, nr. 30, Nota «Naar toegankelijkheid van overheidsinformatie»

24 565, TK 1995–1996, Elektronische snelwegen. – (1–6)

25 266, TK 1996–1997, Bescherming van jeugdigen tegen schadelijke invloeden van audiovisuele media. – (1–4)

25 398, TK 1996–1997, Wijziging van de Wet politieregisters, houdende nadere regels voor bijzondere politieregisters ten behoeve van de politie, Koninklijke marechaussee en daartoe aangewezen diensten van publiekrechtelijke lichamen die met opsporing van strafbare feiten zijn belast (Bijzondere politieregisters)

25 403, TK 1996–1997, Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden)

25 443, TK 1996–1997, Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepalingen inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim. – (A-B, 1–15)

25 533, TK 1996–1997, Regels inzake de telecommunicatie (Telecommunicatiewet). – (A, 1–3)

Mededingingswet, Stb. 1997, 242

Voorontwerp wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met nieuwe ontwikkelingen in de informatietechnologie (Computercriminaliteit II)

Voorstel van wet Wet bescherming persoonsgegevens

Vragen van de leden Van Zuijlen (PvdA) en Roethof (D66) over mogelijke inzage in computerbestanden van internetproviders in verband met emailverkeer van voetbalvandalen, TK 1996–1997, Aanhangsel 1370

Vragen van de leden Rouvoet en Van Dijke (beiden RPF) over het weren van kinderporno op internet, TK 1996–1997, Aanhangsel 1428

Wet computercriminaliteit, Stb. 1993, 33

Wet persoonsregistraties, Stb. 1988, 665

Bijlage 4

Relevante documenten EU

Communication from the Commission: ensuring security and trust in electronic communication: towards a European framework for digital signatures and encryption, COM (97) 503

Gemeenschappelijk standpunt (EG) nr. 57/96 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, met name in het kader van het digitale netwerk voor geïntegreerde diensten (ISDN) en van mobiele digitale netwerken. – PbEG 1996, L315

Global Information Networks: Ministerial Conference Bonn 6–8 July 1997: Ministerial Declaration

Green paper on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation: towards an information society approach, COM (97) .., ip/97/1073

Groenboek inzake de rechtsbescherming van geëncrypteerde diensten op de interne markt, COM (96) 76 def.

Groenboek inzake het auteursrecht en de naburige rechten in de informatiemaatschappij, COM (95) 382 def.

Groenboek leven en werken in de informatiemaatschappij: de mens voorop, COM (96) 389 def.

Groenboek over de bescherming van minderjarigen en de menselijke waardigheid in de context van de audiovisuele en informatiediensten, COM (96) 483 def.

Groenboek inzake de convergentie van de telecomunicatie, media en informatie technologie sectoren en de gevolgen voor regulering. COM (97) 623

Mededeling van de Commissie: de gevolgen van de informatiemaatschappij voor het beleid van de Europese Unie: voorbereiding van de volgende stappen, COM (96) 395 def.

Mededeling van de Commissie: de universele dienst in de telecommunicatiesector in het perspectief van een volledig geliberaliseerde omgeving: een essentieel element van de informatiemaatschappij, COM (96) 73 def.

Mededeling van de Commissie doorzichtigheid van de wetgeving binnen de interne markt voor de diensten van de informatiemaatschappij, COM (96)392 def.

Mededeling van de Commissie: een Europees initiatief op het gebied van de elektronische handel, COM (97) 157 def.

Mededeling van de Commissie: Europa op weg naar de informatiemaatschappij: een actieplan, COM (94) 347 def.

Mededeling van de Commissie: illegale en schadelijke inhoud op het Internet, COM (96) 487 def.

Mededeling van de Commissie inzake normalisatie en de wereldwijde informatiemaatschappij: de Europese aanpak, COM (96) 359 def.

Mededeling van de Commissie over de informatiemaatschappij van Korfoe naar Dublin: de nieuwe prioriteiten, COM (96)395 def.

Mededeling van de Commissie: vervolg op het groenboek inzake het auteursrecht en de naburige rechten in de informatiemaatschappij, COM (96) 568 def.

Mededeling van de Commissie: werk maken van diensten, CSE (96) 6 def.

Ontwerp-overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen Lid-Staten van de Europese Unie. – Document 7945/97 JUSTPEN 41

Richtlijn 89/552/EEG betreffende coördinatie van bepaalde wettelijk en bestuursrechtelijke bepalingen in de Lid-Staten inzake de uitoefening van televisie-omroepactiviteiten. – PbEG 1989, L298

Richtlijn 90/387/EEG betreffende de totstandbrenging van de interne markt voor telecommunicatiediensten door middel van de tenuitvoerlegging van Open Network Provision (ONP). – PbEG 1990, L192

Richtlijn 90/388/EEG betreffende de mededinging op de markten voor telecommunicatiediensten. – PbEG 1990, L192

Richtlijn 91/250/EEG betreffende de rechtsbescherming van computerprogramma's. – PbEG 1991, L122

Richtlijn 93/83/EEG tot coördinatie van bepaalde voorschriften betreffende het auteursrecht en naburige rechten op het gebied van de satelliet-omroep en de doorgifte via de kabel. – PbEG 1993, L248

Richtlijn 94/46/EG tot wijziging Richtlijn 88/301/EEG en Richtlijn 90/388/EEG met name met betrekking tot satellietcommunicatie. – PbEG 1994, L268

Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. – PbEG 1995, L281

Richtlijn 95/47/EG inzake het gebruik van normen voor het uitzenden van televisiesignalen. – PbEG 1995, L281

Richtlijn 95/62/EG inzake de toepassing van «Open Network Provisions» (ONP) op spraaktelefonie. – PbEG 1995, L321

Richtlijn 96/6/EG betreffende de rechtsbescherming van databanken. – PbEG 1996, L77

Richtlijn 97/7/EG betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten. – PbEG 1997, L144

Richtlijn 97/36/EG tot wijziging van Richtlijn 89/552/EEG betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake de uitoefening van televisie-omroepactiviteiten

Tussentijds verslag over de in de EU-lidstaten genomen initiatieven ter bestrijding van illegale en schadelijke inhoud op Internet, SEC (97) 1278

Verdrag betreffende de rechterlijke bevoegdheid en de erkenning en tenuitvoerlegging van beslissingen in burgerlijke en handelszaken (EEX)

Verdrag inzake het recht dat van toepassing is op verbintenissen uit overeenkomsten (EVO), 1980

Voorstel voor een beschikking van de Raad tot aanneming van een communautair meerjarenprogramma om de totstandbrenging van de informatiemaatschappij in Europa te stimuleren (informatiemaatschappij), COM (96) 592 def. (gewijzigd voorstel, COM (97) 460 def.)

Voorstel voor een richtlijn van het Europese Parlement en de Raad betreffende de rechtsbescherming van diensten gebaseerd op, of bestaande uit, voorwaardelijke toegang. – PbEG 1997, C314

Working document of the Commission Services: the Internet Domain Name System and Trademarks, 1997

Bijlage 5

Relevante documenten andere internationale organisaties

1. OESO

Current work on consumer protection in the field of electronic commerce in the OECD coutries, 1997. – DSTI/ICCP(97)18

Follow-up to the report to ministers on GII/GIS and the future work of the Committee, 1997. – DSTI/ICCP(97)17

Implementing the OECD «Privacy guidelines» in the electronic environment: focus on the Internet / Group of experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure, 1997. – DSTI/ICCP/REG(97)6

OECD cryptography policy guidelines ; recommandation of the Council, 1997. – (Http://www.oecd.org/dsti/iccp/crypto_e.html)

OECD global information infrastructures, global information society (GII-GIS): policy recommandations for action, 1997. – DSTI/ICCP (96) 25

OECD global information infrastructures, global information society (GII-GIS): policy requirements, 1997. – DSTI/ICCP (96) 24

OECD guidelines for the security of information systems, 1993

OECD Secretariat consultation paper on international co-operation concerning content and conduct on the Internet, 1997. – DSTI/ICCP (97) 7

2. Raad van Europa

Aanbeveling R(91)14 over de juridische bescherming van televisiediensten

Computer related crime: Recommandation No. R(89)9

Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken, Straatsburg, 20 april 1959, Trb. 1965, 10

Extraterritorial criminal jurisdiction: report of the Council of Europe / European Committee on Crime Problems, 1990

The management of criminal justice: Recommandation No. R(95)12 adopted by the Committee of Ministers of the Coucil of Europe on 11 September 1995

Problems with criminal procedural law connected with information technology: Recommandation No. R(95)13 adopted by the Committee of Ministers on 11 September 1995

Protection of personal dat in the area of telecommunication services with particular reference to telephone services: Recommandation No. R(95)4 adopted by the Committee of Ministers on 7 February 1995

Protecting privacy on the Internet or Guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highways, which may be incorporated in or annexed to Codes of conduct / Project Group on data protection, Strasbourg, 14–17 October 1997

Terms of reference of the Committee of Experts on Crime in Cyber-Space (PC-CY)

Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens; Straatsburg, 28 januari 1981. – Tractatenblad 1988, nr. 7

3. VN

UNCITRAL Model Law on electronic commerce, 1996

United Nations manual on the prevention and control of computer-related crime. – New York, 1994. – International review of criminal policy 1994, nos. 43 and 44

4. WIPO

Draft treaty on intellectual property rights in respect of databases

WIPO Copyright Treaty (CRNR/OC/95)

WIPO Performances and Phonograms Treaty (CRNR/OC/95)

5. International Chamber of Commerce

ICCGuidelines on interactive marketing communications: principles for respnsible commercial communications over the Internet, World Wide Web, Online services and electronic networks (concept) / Dept. for International Commercial Policy and Techniques. – Paris, 6 June 1996. – Doc. no. 240–44/4 rev 5

Bijlage 6

Overzicht van belangrijke projecten op het gebied van informatie- en communicatietechnologie

1. De rijksoverheid

Het kabinet heeft in 1995 het Nationaal Actieprogramma elektronische snelweg geïntroduceerd. Dit actieplan bevat actielijnen waarmee het kabinet de ontwikkeling van de elektronische snelweg wil stimuleren en de belemmeringen wil wegnemen. De invulling van die lijnen geschiedde grotendeels met reeds bestaande projecten of projecten die in voorbereiding zijn. Het NAP voorziet de diverse projecten van een overkoepelend geheel en onderlinge samenhang.

Naam project	Uitvoering	Omschrijving	Aard project en producten
Informatietechno-logie en Recht	ITeR (EZ en OC&W, Just, V&W, BiZa)	Onderzoek naar samenhang in de juridische implicaties van de veranderingen die zich op het terrein van de IT voltrekken.	Onderzoeks-programma, beleids-voorbereiding. Publicaties, workshops en conferenties
Auteursrecht, naburige rechten en nieuwe media	Just, OC&W	Positiebepaling van Nederland in de nationale en internationale (EU, WIPO) discussie over de toekomst van het auteursrecht	Notitie voor de Tweede Kamer
Dematerialisering de economie; over mobiliteit, communicatie en informatie.	WRR	Dit project richt zich op diverse onderwerpen: – belastingheffing; – veranderingen in economische structuur; – territorialiteit als basis van wet- en regelgeving; – transport van economische waarde; – geografische verbrokkeling van bedrijfskolommen.	Beleidsvoorbereiding. Voorstudie en rapport aan kabinet
Privacy	Rathenau Instituut	Doel van het project is de privacy-discussie een nieuwe impuls te geven.	Beleidsvoorbereiding. Discussiestuk Tweede Kamer
Gevolgen van ICT-ontwikkelingen voor het openbaar bestuur	BiZa/ Raad voor het Openbaar Bestuur	Een tweetal adviezen worden gevraagd: – Advies over veranderingen a.g.v. ICT-ontwikkelingen, voor het openbaar bestuur. – Gevolgen van ICT voor de Grondwet.	Beleidsvoorbereiding. Advies aan minister van BiZa
Informatietechnologie en Ethiek	NWO/ Bureau Ethiek en Beleid, Erasmus Universiteit	De ethische kanten van het onderwerp «Privacy tussen Individu en Gemeenschap»	Beleidsvoorbereiding. Onderzoeksrapport voor beleidsmakers
De consument op nieuwe markten	SER, Commissie voor Consumenten-aangelegenheden	Vanuit het perspectief van marktpartijen toetsen van juridische randvoorwaarden voor consumententransacties op hun bruikbaarheid in situaties waarin deze transacties langs elektronische weg tot stand komen.	Advisering. Voor eigen gebruik
TTP's	V&W/EZ	Identificeren van condities waaronder een infrastructuur voor informastiebeveiligingsdiensten kan worden gerealiseerd	Notitie voor de Tweede Kamer
Actieplan Electronic commerce	EZ	Ontwikkelen van Nederland tot toonaangevend land op het gebied van electronic commerce en information gateway to Europe	Notitie voor de Tweede Kamer
Notitie Publiek Domein	OC&W	Uitvoeringsactielijn 3 NAP	
Algemeen bereik van informatiediensten	OC&W, Tijdelijke Commissie Informatiebeleid	Advies over de rol van de overheid bij het voorkomen van scheidslijnen in de toegankelijkheid van informatie.	Advies aan het kabinet
Post en marktwerking	V&W	Een onderzoek naar de wenselijkheid, noodzaak en effecten van de huidige post-concessie	Beleidsvoorbereiding

2. De Europese Unie

In het kader van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie heeft de Europese Unie een Permanent Actieplan opgezet. Dit plan heeft als doel de verschillende nationale maatregelen in goede banen te leiden en eventueel te versnellen.

Nederlandse departementen die betrokken zijn bij de uitvoering van het actieplan zijn het Ministerie van Economische Zaken, het Ministerie van Verkeer en Waterstaat, het Ministerie van onderwijs, Cultuur en Wetenschap, het Ministerie van Binnenlandse Zaken en het Ministerie van Justitie, eventueel het Ministerie van Sociale Zaken en Werkgelegenheid en het Ministerie van Financiën.
Voor een volledig overzicht van initiatieven en beleidsdocumenten van de Europese Unie – voorzover niet in deze nota genoemd en niet opgenomen in bijlage 4 (Relevante documenten EG) wordt verwezen naar de website van het ISPO (Information Society Project Office): http://www.ispo.cec.be

3. De Organisatie voor Economische Samenwerking en Ontwikkeling

3.1. Informatie- en communicatiebeleid

ICCP-Committee (Information, Computer and Communications Policy) van de OECD analyseert infrastructuur-voorstellen van nationale overheden en internationale organisaties en standaard prestatie-indicatoren.
Voornaamste publicaties in dit kader zijn de jaarlijkse *Information technology Outlook*, *Communications Outlook* en de *Telecommunications Database.* Andere publicaties en/of activiteiten:
- OCDE/GD(97)207: rapport *Internet Domain Name: Allocation Politics*.
- OCDE/GD(97)221: rapport: *Webcasting and Convergence: Policy Implications*. Onderwerp: problemen van regulering bij convergentie van technieken.

3.2. Informatie economie

- Serie workshops over de informatie economie tussen juni 1995 en maart 1997. Onderwerpen: Stock-taking (Toronto, juni 1995), Netwerk economie (Istanbul 1995), Elektronische handel (Tokio, 1996), Human resources en informatiesamenleving (Porvoo, 1996), Overheidsrespons op informatiesamenleving (Seoul, 1996) en concurrentie en innovatie (Londen 1997). Summary reports zijn op de OESO-site beschikbaar.
- Turku-conferentie (Turku, Finland, november 1997), internationale conferentie over het wegnemen van belemmeringen voor internationale elektronische handel. Eindrapport inmiddels beschikbaar.
- OCDE/GD(97)185: rapport *Measuring Electronic Commerce*. Doel: ontwikkelen meetinstrumenten en randvoorwaarde om (vergelijkend) onderzoek naar elektronische handel te kunnen doen.
- Sacher-rapport (juni 1997). Onder voorzitterschap van John Sacher (pres. Marks and Spencer) is een rapport totstand gekomen over noodzakelijke voorwaarden voor elektronische handel.

3.3. Informatiebeveiliging en privacy

DE OESO ontwikkelt instrumenten die de basis kunnen zijn voor wetgeving, standaardisatie en het ontwikkelen van technische criteria.
Belangrijke activiteiten en/of documenten in dit kader:
- 1980 OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- 1985 Declaration on Transborder Data Flows
- 1992 OECD Guidelines for the Security of Information Systems
- (Vanaf 1992) zijn verschillende conferenties over cryptografie georganiseerd teneinde te komen tot internationaal vergelijkbare criteria voor cryptografie-beleid. In maart 1997 werden richtlijnen vastgesteld: 1997 OECD Cryptography Policy Guidelines

3.4. Telecommunicatie en informatiediensten

De OESO onderzoekt met name gevolgen van convergentie van omroep, telecommunicatie en informatica en economische aspecten en regulering van informatie-inhoud. In 1997 keurden de OESO-ministers het rapport *Global Onformation Infrastructure-Global Information Society* goed; dit rapport bevat voorstellen voor stimuleren van ontwikkeling van multimedia-diensten.

4. De Raad van Europa

De European Committee on Crime Problems (CDPC) heeft in januari 1997 besloten een Committee of Experts on Crime in Cyber-Space (PC-CY) in te stellen. De opdracht is om een bindende regeling op te stellen en daartoe de volgende onderwerpen te onderzoeken:

1. «Cyberspace-misdaden», gepleegd door middel van het gebruik van telecommunicatienetwerken, zoals illegale geldtransacties, aanbieden van illegale diensten, inbreuken op het auteursrecht, inbreuken op de menselijke waardigheid e.d.;
2. Andere strafrechtelijke thema's waar een gemeenschappelijke aanpak nodig is voor het doel van de internationale samenwerking, zoals definities, straffen en aansprakelijkheid van de actoren in cyberspace;
3. Het (grensoverschrijdende) gebruik en de toepasbaarheid van dwangmiddelen in een technologische omgeving, bijvoorbeeld onderschepping van telecommunicatie, elektronische surveillance van informatienetwerken, opsporing en inbeslagneming in informatieverwerkende systemen, ontoegankelijkmaking van strafbare informatie, medewerkingsverplichting voor serviceproviders vooral waar het beveiliging en encryptie betreft;
4. Het probleem van de rechtsmacht in verband met de «cyberspace-misdaden», bijvoorbeeld het bepalen van de plaats waar het strafbare feit is gepleegd. Hieruit moet immers blijken welk nationaal recht er vervolgens toepasselijk is, waarbij ook rekening gehouden moet worden met het ne bis in idem-beginsel mochten er meerdere rechtsmachten toepasselijk worden geacht en hoe er vermeden kan worden dat er een rechtsmachtvacuüm ontstaat.

HOOFDSTUK 2 ALGEMENE ONDERWERPEN VAN REGELGEVING

§ 2.1 Gebruik van regelgeving

Aanwijzing 6

1. Tot het tot stand brengen van nieuwe regelingen wordt alleen besloten, indien de noodzaak daarvan is komen vast te staan.
2. Met het doen van uitspraken en toezeggingen over nieuwe regelingen wordt grote terughoudendheid betracht.

Toelichting:

Terughoudendheid met het doen van uitspraken en toezeggingen over nieuwe regelgeving is onder alle omstandigheden geboden. Zij is echter volstrekte noodzaak, indien nog niet vaststaat dat een dergelijke uitspraak of toezegging gestand kan worden gedaan of duidelijk is welke lasten met de nieuwe regeling gemoeid zijn.

Aanwijzing 7

Alvorens tot het treffen van een regeling wordt besloten, worden de volgende stappen gezet:

a. kennis wordt vergaard van de relevante feiten en omstandigheden met betrekking tot het bewuste onderwerp;
b. de doelstellingen die worden nagestreefd, worden zo concreet en nauwkeurig mogelijk vastgesteld;
c. onderzocht wordt of de gekozen doelstellingen kunnen worden bereikt door middel van het zelfregulerend vermogen in de betrokken sector of sectoren dan wel daarvoor overheidsinterventie noodzakelijk is;
d. indien overheidsinterventie noodzakelijk is, wordt onderzocht of de gekozen doelstellingen kunnen worden bereikt door aanpassing of beter gebruik van bestaande instrumenten dan wel, indien dit niet mogelijk blijkt, welke andere mogelijkheden daartoe bestaan;
e. de diverse mogelijkheden worden zorgvuldig tegen elkaar afgewogen.

Toelichting:

Onderdeel a: Kennis feiten en omstandigheden. Kennis van de relevante feiten en omstandigheden is noodzakelijk om tot een verantwoorde besluitvorming te kunnen komen.
Allereerst moet de betrokken kennis worden gebruikt voor het formuleren van de doelstellingen. Vervolgens is zij nodig voor de beantwoording van de vraag in hoeverre overheidsinterventie nodig is en voor de afweging van de verschillende mogelijkheden tot overheidsinterventie. Gewoonlijk vindt het verzamelen van de gegevens overigens gefaseerd plaats. Voor elke nieuwe stap in het besluitvormingsproces zijn veelal weer nieuwe (meer gedetailleerde) gegevens nodig.

Onderdeel b: Nauwkeurige doelstellingen. Een zo concreet en nauwkeurig mogelijke vaststelling van doelstellingen houdt in dat verschillende doelstellingen duidelijk worden onderscheiden. Waar dat mogelijk en relevant is, dient ook te worden vastgesteld binnen welke termijn ernaar wordt gestreefd een doelstelling te bereiken. Indien kwantificering, financieel of anderszins, van een doelstelling mogelijk is, dient deze ook te geschieden.

Onderdeel c: Noodzaak overheidsinterventie. Slechts voor zover het zelfregulerend vermogen van de maatschappij tekortschiet, moet worden gedacht aan overheidsmaatregelen. Zie voor een voorbeeld van (wettelijk geconditioneerde) zelfregulering: artikel 26, vijfde lid, van de Wet op het consumentenkrediet. Zie verder aanwijzing 8.

Onderdeel d: Alternatieven overheidsinterventie. Bij het onderzoek naar de mogelijkheden die de overheid ten dienste staan om een doelstelling te bereiken, dienen de verschillende denkbare alternatieven de revue te passeren. Het gaat daarbij evenzeer om instrumenten die door middel van wetgeving worden gecreëerd, zoals ge- en verboden, een vergunningenstelsel en een heffingenstelsel, als om andere middelen, zoals feitelijk optreden van de overheid en subsidies. Overigens brengt het uitgangspunt van de rechtsstaat mee dat ten aanzien van deze andere middelen, in verband met het bieden van rechtswaarborgen, veelal ook wettelijke voorzieningen moeten worden getroffen.
Het onderzoek naar de mogelijkheden tot overheidsinterventie kan overigens ook tot de slotsom leiden dat de overheid de betrokken doelstellingen niet kan realiseren. Dan moet van overheidsinterventie worden afgezien.
Wat wettelijke regelingen betreft kunnen te onderzoeken varianten zowel betrekking hebben op de opzet van een wettelijke regeling als zodanig als op onderdelen van een regeling (bij voorbeeld het systeem van rechtsbescherming waarvoor wordt gekozen).

Overigens zij opgemerkt dat het van de aard van het betrokken geval zal afhangen of de in deze aanwijzing bedoelde onderzoeken omvangrijk dienen te zijn of heel beperkt van aard kunnen blijven. Het is echter wel noodzakelijk dat de in deze aanwijzing bedoelde stappen in alle gevallen waarin het treffen van een regeling een van de mogelijkheden is, worden gezet.

Aanwijzing 8

Bij het bepalen van de keuze voor een mogelijkheid tot overheidsinterventie om een doelstelling te bereiken wordt zoveel mogelijk aangesloten bij het zelfregulerend vermogen in de betrokken sector of sectoren.

Toelichting:
Indien het zelfregulerend vermogen van de maatschappij tekortschiet om een doelstelling te bereiken, dient te worden bezien of dit vermogen door overheidsmaatregelen kan worden versterkt. Direct overheidsingrijpen is slechts op zijn plaats, indien van het zelfregulerend vermogen van de maatschappij – ook versterkt met ondersteunende overheidsmaatregelen – niet voldoende resultaten te verwachten zijn.

Aanwijzing 9

Bij de afweging van verschillende mogelijkheden tot overheidsinterventie om een doelstelling te bereiken wordt in ieder geval gelet op de volgende aspecten:
a. de mate waarin verwacht mag worden dat een regeling het beoogde doel zal helpen te verwezenlijken;
b. de neveneffecten van een regeling;
c. de lasten van een regeling voor de overheid enerzijds en burgers, bedrijven en instellingen anderzijds.

Toelichting:

Onderdeel a: Effectiviteit. Wat het onder a bedoelde aspect betreft verdienen bij een overwogen regeling onder meer de uitvoerbaarheid en de te verwachten mate van naleving ervan aandacht. Aandachtspunt moet daarbij ook de mogelijkheid tot handhaving zijn. In het oog dient in dit verband te worden gehouden dat naar mate de in een regeling vervatte normen en bestuurlijke instrumenten voor de justitiabelen minder vanzelfsprekend zijn, de naleving – en bijgevolg ook de handhaving – daarvan problematischer is. Zie ten aanzien van de handhaving verder aanwijzing 11.

Onderdeel b: Neveneffecten. Met betrekking tot het onder b bedoelde aspect zij het volgende opgemerkt. Is er sprake van een beoogd neveneffect, dan is een (secundaire) doelstelling van de regeling in het geding. Deze dient dan ook als zodanig te worden

aangewezen. Bij onbedoelde neveneffecten moet worden bezien in hoeverre deze de aanvaardbaarheid van een regeling niet negatief beïnvloeden. Negatieve beïnvloeding kan aanleiding zijn van een regeling af te zien. Anderzijds dient slechts tot het tot stand brengen van een regeling te worden besloten indien zij geschikt lijkt de gekozen doelstelling(en) te realiseren. Er is sprake van een onzuivere afweging indien positieve maar onbedoelde neveneffecten de doorslag zouden geven om een regeling in te voeren die onvoldoende adequaat lijkt voor het verwezenlijken van de gekozen doelstelling(en).
Welke de negatieve neveneffecten van een maatregel zullen zijn, moet steeds in breed verband worden onderzocht. Aandacht verdient daarbij onder meer ook in hoeverre een maatregel van verstorende invloed zal zijn op het effect dat bestaande regelingen hebben. De werking van een regeling kan worden verstoord doordat een nieuwe regeling het voor de justitiabele minder aantrekkelijk maakt aan eerstbedoelde regeling te voldoen. Voorts kan een nieuwe regeling naast reeds bestaande regelingen tot gevolg hebben dat een zodanige cumulatie van verplichtingen ontstaat dat de bereidheid tot naleving van de betreffende regelingen afneemt.

Gevolgen voor sociaal-economische ontwikkeling. Met name dient verder steeds te worden bezien welke gevolgen voor de sociaal-economische ontwikkeling direct of indirect uit een maatregel kunnen voortvloeien. Hierbij kan onder meer worden gedacht aan gevolgen voor de concurrentiepositie van het bedrijfsleven (nationaal en internationaal), de flexibiliteit van de markt, de afzetontwikkeling (binnenlandse en buitenlandse markt), de werkgelegenheid, de rentabiliteit van ondernemingen, de investeringsgeneigdheid en de beloningsstructuur.
Bedacht moet verder worden dat het overgaan tot overheidsingrijpen op een tot dusver door de overheid niet betreden terrein nogal eens het begin inhoudt van een langdurig proces van in intensiteit toenemende overheidsbemoeienis, dat leidt tot maatschappelijke verstarringen. Zulke verstarringen zijn vaak slechts ten koste van grote inspanningen ongedaan te maken.

Onderdeel c: Uitvoeringslasten. Wat het onder c bedoelde aspect betreft zij verder verwezen naar de aanwijzingen 13, 14 en 15.

Tot slot zij vermeld dat ten aanzien van de verschillende te overwegen mogelijkheden tot overheidsinterventie de onder a, b en c bedoelde aspecten alle in onderlinge samenhang onder de loep dienen te worden genomen.

Aanwijzing 10

1. Gestreefd wordt naar duidelijkheid en eenvoud van regelingen en naar een bestendig karakter daarvan.
2. Indien een regeling bij wijze van experiment dient te worden ingevoerd, wordt het tijdelijk karakter in de regeling tot uitdrukking gebracht.

Toelichting:

Eerste lid: Bestendigheid van regelingen. Een regeling is bestendig indien zij niet frequent behoeft te worden gewijzigd. Het verdient aanbeveling naar zo groot mogelijke bestendigheid van regelingen te streven. Dit betekent dat het beleid in beginsel duidelijk moet zijn alvorens tot het treffen van een regeling wordt overgegaan.

Tweede lid: Experimentele regelingen. Een en ander laat onverlet dat soms behoefte bestaat aan regelingen met een experimenteel karakter. Tot een dergelijke regeling moet overigens niet te snel worden overgegaan. In bepaalde gevallen moet de wetgever tot het nemen van maatregelen besluiten zonder dat geheel kan worden overzien wat de effecten daarvan zullen zijn. Het kan ook aangewezen zijn om, terwijl een wet in hoofdzaak blijft gelden, in bepaalde regio's dan wel ten aanzien van bepaalde personen of instellingen een ander dan het in de wet neergelegde beleid te voeren met het oog op een overwogen wijziging van de wet. Aan een dergelijke experimentele regeling dient wel een tijdelijk karakter te worden gegeven. Zie in dit verband de aanwijzingen 181 tot en met 183.

Aanwijzing 11

1. Tot het treffen van een regeling wordt niet besloten dan nadat is nagegaan of in voldoende mate handhaving te realiseren valt.
2. Hierbij wordt onderzocht of handhaving het beste langs bestuursrechtelijke, privaatrechtelijke of strafrechtelijke weg dan wel op andere wijze kan plaatsvinden.

Toelichting:

Eerste lid: Handhavingsmogelijkheden. Voor het realiseren van een met een regeling beoogde doelstelling is onontbeerlijk dat de regeling wordt gehandhaafd. Of handhaving in voldoende mate mogelijk is, dient derhalve te worden onderzocht voordat tot het treffen van de regeling wordt besloten. In het bijzonder geldt dit indien de regeling ge- of verboden bevat, maar ook in andere gevallen – bij voorbeeld met betrekking tot voorschriften die aan een vergunning worden verbonden – is het handhavingsaspect van betekenis.
Uit het onderzoek moet blijken welke inspanningen nodig worden geacht voor de preventieve en repressieve handhaving ervan. Bij wetsvoorstellen die uit een oogpunt van uitvoering en handhaving ingrijpende veranderingen tot gevolg hebben, worden die bevindingen neergelegd in handhaafbaarheids- en uitvoerbaarheidsrapporten. Over de handhavingsmogelijkheden moet reeds voordat tot het treffen van de regeling wordt besloten worden overlegd tussen de ontwerpers van de beoogde regeling en de instanties die met de uitvoering en handhaving van de regeling zullen worden belast.
De volgende aspecten zijn bij de beoordeling van de handhaafbaarheid in ieder geval van belang:
– een regel moet zo weinig mogelijk ruimte laten voor interpretatiegeschillen;
– uitzonderingsbepalingen moeten tot een minimum worden beperkt;
– regels moeten zo veel mogelijk zijn gericht op zichtbare dan wel objectief constateerbare feiten;
– regels moeten werkbaar zijn voor degene tot wie de regels zijn gericht en voor de personen die met handhaving zijn belast.

Tweede lid: Handhavingsmethoden. In dit verband moeten ook de verschillende handhavingsmethoden tegen elkaar worden afgewogen. Daarbij valt in de eerste plaats te denken aan bestuursrechtelijke, privaatrechtelijke en strafrechtelijke middelen. Ook kan echter gedacht worden aan de mogelijkheden die het tuchtrecht biedt en aan preventieve middelen zoals voorlichting. Voor elk van de repressieve handhavingsmethoden dient verder aandacht te worden besteed aan de mogelijke sancties. Bij de afweging van de verschillende mogelijkheden dienen de aspecten, bedoeld in aanwijzing 9, aan de orde te komen. In bepaalde gevallen is het aangewezen niet voor één handhavingsmethode te kiezen maar voor een combinatie van verschillende methoden. Overigens dient ervoor te worden gewaakt dat niet zonder noodzaak wordt voorzien in een cumulatie van sanctiemogelijkheden voor de handhaving van één verplichting.
Een keuze voor het strafrecht valt in het algemeen slechts te rechtvaardigen indien aannemelijk wordt gemaakt dat bestuursrechtelijke, privaatrechtelijke en tuchtrechtelijke oplossingen te kort schieten. Bestuursrechtelijke handhaving kan een goed alternatief bieden, mits aan de eisen die uit artikel 6 van het Europees Verdrag tot bescherming van de Rechten van de mens en de fundamentele vrijheden volgen, wordt voldaan. Zie verder ook aanwijzing 139. Indien toch wordt gekozen voor strafrechtelijk te sanctioneren bepalingen, vereist de formulering van de elementen van de delictsomschrijvingen bijzonder veel zorg (zie aanwijzing 144). Hierover moet in voorkomende gevallen worden overlegd met het Ministerie van Justitie of rechtstreeks met het openbaar ministerie.

Bij het in deze aanwijzing bedoelde onderzoek moet in het oog worden gehouden dat de justitiële en bestuurlijke handhavingscapaciteit beperkt is.

Aanwijzing 12

Een regeling wordt op zodanige wijze ingericht dat zij zo weinig mogelijk conflicten oproept. Daartoe wordt onder meer aan het volgende voldaan:

a. het aantal beslismomenten waartoe toepassing van de regeling aanleiding geeft, wordt tot een minimum beperkt;
b. ingeval administratieve boetes mogelijk worden gemaakt, worden daarvoor bindende tarieven vastgesteld;
c. de aard en omvang van uitkeringen, voorzieningen en andere voordelen worden zo duidelijk mogelijk in algemeen verbindende voorschriften of goed kenbaar gemaakte beleidsregels omschreven.

Toelichting:

Noodzaak conflictbeperking. Tot op zekere hoogte is het onvermijdelijk dat regelingen waarbij aan de burger lasten worden opgelegd of die hem aanspraak geven op bepaalde voordelen, aanleiding geven tot conflicten. Het is echter gewenst dat deze conflicten tot een minimum worden beperkt. Deze wenselijkheid is er allereerst vanuit een sociaal-maatschappelijk oogpunt. Daarnaast is beperking van het aantal conflicten gewenst om de lasten die verbonden zijn aan de rechtsbescherming ter zake van de toepassing van de regeling, zo laag mogelijk te houden.
Gelet hierop dient bij de keuze uit varianten van een regeling ook de mate waarin over de toepassing daarvan conflicten zijn te verwachten, in beschouwing te worden genomen.

Conflictopwekkende factoren. Onder meer zijn regelingen in bijzondere mate conflictopwekkend indien zij een van de volgende kenmerken vertonen:

– het verkrijgen van een uitkering, een voorziening, een restitutie of een ander voordeel wordt afhankelijk gesteld van individueel bepaalde omstandigheden zoals het hebben van een ziekte of gebreken dan wel het zijn van ondernemer;
– belanghebbenden worden met een reeks van beschikkingen geconfronteerd;
– aan een uitvoeringsorgaan wordt een ruime mate van discretionaire bevoegdheid gelaten;
– voor het bepalen van de hoogte van een uitkering of van de aard van een voordeel worden slechts vage normen gesteld;
– het verkrijgen van een uitkering of van een voordeel dan wel de verplichting om belasting of een heffing te betalen wordt bepaald door een groot aantal persoonlijke omstandigheden waarvan moet blijken uit door het uitvoeringsorgaan te verifiëren gegevens die de betrokkene verstrekt;
– de besluitvorming omtrent het toekennen van uitkeringen of andere voordelen vindt plaats nadat andere organen dan de met de besluitvorming belaste instantie een extern advies hebben uitgebracht dat aan betrokkene bekend wordt gemaakt, maar waarvan de met de besluitvorming belaste instantie nog mag afwijken;
– er worden gunstige besluiten met een voorlopig karakter genomen, die worden gevolgd door mindere gunstige;
– aan een orgaan dat bevoegd wordt verklaard tot het opleggen van administratieve sancties, worden ruime grenzen gelaten om de aard en de omvang van de sancties te bepalen.

Wat fiscale regelgeving betreft zijn verder onder meer nog in het bijzonder conflict-opwekkend regelingen die een van de volgende elementen bevatten:

– een financieel belang wordt verbonden aan bijzondere, niet strikt te omschrijven omstandigheden;
– ontwikkelingen in vele uiteenlopende en betrekkelijk smalle sectoren van het maatschappelijk leven worden door middel van het fiscale instrument overmatig gestuurd;
– doelgroepen worden onduidelijk afgebakend.

Zie met betrekking tot onderdeel c ook aanwijzing 24, tweede lid.

Aanwijzing 13

Bij de keuze voor een bepaalde regeling wordt gestreefd naar zo beperkt mogelijke lasten voor burgers, bedrijven en instellingen, voor zover niet uitdrukkelijk het opleggen van lasten wordt beoogd.

Toelichting:

Lasten voor burgers. Wat de gevolgen voor burgers betreft kan worden gedacht aan administratieve verplichtingen, de noodzaak tot inschakeling van deskundigen, het vertragend effect van termijnen en nieuwe rechtstreekse financiële lasten die uit een regeling voortvloeien.

Lasten voor bedrijven en instellingen. Voor het bedrijfsleven en non-profitinstellingen verdienen de aandacht:
a. gevolgen voor het besluitvormingsproces binnen de onderneming of instelling, zoals die voortvloeien uit bepalingen inzake medezeggenschap en overleg;
b. gevolgen voor ondernemingen of instellingen die voortvloeien uit het besluitvormingsproces bij de overheid, bij voorbeeld in verband met onzekerheid omtrent en tijdsbeslag van overheidsbeslissingen, dan wel in verband met inspraak of beroep;
c. gevolgen voor de organisatie van de onderneming of instelling, zoals de noodzaak voorzieningen te treffen om te voldoen aan administratieve verplichtingen of om de benodigde deskundigheid in te schakelen;
d. gevolgen voor de bedrijfsvoering binnen de onderneming of instelling, zoals veiligheidseisen, eisen met betrekking tot het te fabriceren of te verhandelen product of met betrekking tot de te verlenen dienst, dan wel eisen die van invloed zijn op de innovatiegeneigdheid;
e. nieuwe rechtstreekse financiële lasten die uit een regeling voortvloeien;
f. wat het bedrijfsleven betreft, gevolgen voor de positie van de ondernemers op de markt, bij voorbeeld ten gevolge van maatregelen die de prijs beïnvloeden, export- en importbeperking, ge- of verbruikersbeperkingen of regels met betrekking tot mededinging.
Lasten voor het bedrijfsleven dienen zowel in ogenschouw te worden genomen met betrekking tot ondernemingen waarop een regeling rechtstreeks betrekking heeft, als ten aanzien van andere sectoren van het bedrijfsleven die gevolgen van een regeling ondervinden.

Aanwijzing 14

Bij de keuze voor een bepaalde regeling wordt eveneens gestreefd naar zo beperkt mogelijke lasten voor de overheid.

Toelichting:

Bij lasten voor de overheid kan worden gedacht aan:
a. lasten die rechtstreeks zijn gemoeid met de uitvoering van de regeling (voorlichting, het behandelen van aanvragen voor vergunningen en ontheffingen, de inning van belastingen en heffingen en de uitvoering van in de regeling voorgeschreven feitelijke handelingen);
b. lasten die voortvloeien uit in de regeling vervatte procedurele voorschriften, zoals voorschriften inzake verplichte advisering, inspraak, vormen van preventief toezicht, planning, verslagleggingsverplichtingen en evaluatieverplichtingen;
c. lasten die verband houden met het toezicht op de naleving en met de handhaving van de regeling (wat de handhaving betreft gaat het om lasten in verband met onder meer de van overheidswege gefinancierde rechtshulp, het openbaar ministerie, de politie, het gevangeniswezen, andere justitiële diensten en de rechtspraak);
d. lasten die voortvloeien uit de rechtsbescherming (lasten in verband met de van overheidswege gefinancierde rechtshulp, met de behandeling van bezwaarschriften en met de rechtspraak en lasten voor uitvoerende instanties als gevolg van procedures).

De onder b bedoelde lasten kunnen onder meer worden beperkt door te streven naar soberheid in procedurele voorschriften en naar een duidelijke toedeling en afbakening van bestuurlijke bevoegdheden zowel op centraal als op decentraal niveau. Bij toedeling van bevoegdheden aan decentraal niveau zijn met name bemoeienis van hoger niveau met de uitoefening van deze bevoegdheden (bij voorbeeld preventief toezicht) en verplichtingen van het decentrale niveau jegens hoger niveau ter zake (bij voorbeeld verplichte verslaglegging) zoveel mogelijk te vermijden.

Bij het maken van een keuze tussen verschillende varianten voor een regeling kan het noodzakelijk zijn lasten voor de overheid af te wegen tegen lasten voor de burger. Het brengen van meer doelstellingen binnen een regeling kan de uitvoering van die regeling ingewikkelder maken en daarmee de voor de overheid met die regeling gemoeide lasten doen toenemen. Aan de andere kant zal het voor de burger vaak belastender zijn om met diverse naast elkaar werkende regelingen te worden geconfronteerd dan met één geïntegreerde regeling.

Aanwijzing 15

De voor een of meer belanghebbenden nadelige gevolgen van een regeling mogen niet onevenredig zijn in verhouding tot de met de regeling te dienen doelen.

Toelichting:

Deze aanwijzing correspondeert met artikel 3: 4, tweede lid, Algemene wet bestuursrecht.

Aanwijzing 16

Taken en bevoegdheden worden op decentraal niveau gelegd, tenzij het onderwerp van zorg niet op doelmatige en doeltreffende wijze door decentrale organen kan worden behartigd.

Toelichting:

Territoriale decentralisatie. Als uitgangspunt geldt dat, indien taken op doelmatige en doeltreffende wijze kunnen worden verricht door besturen van provincies, gemeenten of waterschappen, zij niet behoren te worden opgedragen aan het Rijk. Evenzeer behoren taken die op doelmatige en doeltreffende wijze door besturen van gemeenten of waterschappen kunnen worden verricht, niet te worden opgedragen aan de besturen van provincies.

Algemeen of functioneel bestuur. Tevens zal per geval moeten worden afgewogen of territoriale dan wel bij voorbeeld gezien de aard van de betrokken taak of de schaal, waarop deze behartigd dient te worden – functionele decentralisatie het meest in aanmerking komt. Uitgangspunt hierbij is dat het zwaartepunt van de politieke en bestuurlijke activiteit berust bij organen van algemeen bestuur (Rijk, provincies en gemeenten). Functioneel bestuur kan onder omstandigheden een goede aanvulling bieden op het algemeen bestuur. Zie inzake organen van functioneel bestuur (zelfstandige bestuursorganen) § 4.5a van deze aanwijzingen.

Aanwijzing 17

1. Bij de toekenning van bestuursbevoegdheden wordt de uitoefening daarvan zoveel mogelijk genormeerd.
2. Met het oog hierop worden discretionaire bevoegdheden en bevoegdheden met vage toepassingscriteria niet toegekend, tenzij daarvoor goede gronden zijn.

Toelichting:

Ten einde de burger voldoende rechtswaarborgen te bieden, moeten bestuursbevoegdheden zo nauwkeurig mogelijk wettelijk worden ingekaderd. Dit geldt evenzeer voor bestuursinstrumenten die de overheid op zich ook zonder wettelijke grondslag zou kunnen hanteren (bij voorbeeld het verlenen van incidentele subsidies). Zie ook aanwijzing 12.
Met het oog op de wenselijkheid rechtswaarborgen te bieden dient ook ten aanzien van elke bevoegdheid te worden bezien in welke mate rechtsbescherming noodzakelijk is. Daarbij geldt als uitgangspunt het in de Algemene wet bestuursrecht neergelegde stelsel van rechtsbescherming. Zie verder de aanwijzingen 148 tot en met 160.

Aanwijzing 18

Bij het ontwerpen van regelingen wordt onderzocht welke hogere regels de vrijheid van regeling ten aanzien van het betrokken onderwerp hebben ingeperkt.

Toelichting:

Bij hogere regels kan het gaan om internationale of communautaire regels, grondwettelijke voorschriften, rechtsbeginselen en – bij regelingen die worden vastgesteld bij algemene maatregel van bestuur of ministeriële regeling – regels die zijn neergelegd in een wet in formele zin. Wat de internationale regels betreft is in het bijzonder te denken aan de Europese regelgeving, het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en het Internationaal Verdrag inzake burgerrechten en politieke rechten. Van de rechtsbeginselen kunnen met name worden genoemd het rechtszekerheidsbeginsel, het gelijkheidsbeginsel en het evenredigheidsbeginsel. Wat de regels aangaat die zijn neergelegd in een wet, dient niet alleen te worden gelet op de wet waarop de betrokken algemene maatregel van bestuur of ministeriële regeling berust, maar ook op andere wetten.