Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1998–1999

# 26 671 Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II)

**Nr. 3**

## MEMORIE VAN TOELICHTING

### Inhoudsopgave



KST36386
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 1999

## ALGEMEEN DEEL

### 1. Inleiding en hoofdlijnen

Het ontstaan en de ontwikkeling van de computer had en heeft ingrijpende gevolgen voor het strafrecht. De Wet computercriminaliteit (Stb. 1993, 33) was het resultaat van een eerste verkenning, naar de toenmalige stand van de techniek, van die gevolgen. In de afgelopen jaren heeft de informatietechnologie zich op stormachtige wijze verder ontwikkeld. In het bijzonder nieuwe technologieën die het mogelijk maken om computers aan elkaar te koppelen en netwerken van computers aan andere netwerken, bieden burgers en overheden ongekende mogelijkheden tot overdracht, verkrijging en bewerking van informatie.
De informatisering van de maatschappij laat de rol van de overheid niet onberoerd. Enerzijds worden de mogelijkheden van de overheid tot controle en sturing, zeker in nationaal verband, kleiner, anderzijds brengt de verantwoordelijkheid van de overheid voor een ordelijk verloop van het verkeer tussen burgers mee dat zij die ordening aanpast aan de gewijzigde omstandigheden opdat ieders gerechtvaardigde belangen zo veel mogelijk juridische bescherming blijven behouden. Dit heeft geleid tot een discussie over de rol van de wetgever op de elektronische snelweg. In februari 1998 heeft mijn ambtsvoorganger namens het kabinet aan de Tweede Kamer een nota over dit onderwerp aangeboden («Wetgeving voor de elektronische snelweg», kamerstukken II 1997/98, 25 880, nrs. 1–2). Uiteraard is bij het opstellen van dit wetsvoorstel rekening gehouden met de in deze nota neergelegde uitgangspunten en (beleids)voornemens.
De Wet computercriminaliteit dient een vervolg te krijgen. Het Wetboek van Strafrecht (Sr) en het Wetboek van Strafvordering (Sv) dienen op verschillende onderdelen te worden aangepast aan de nieuwe ontwikkelingen in de informatietechnologie. Dit wetsvoorstel strekt daartoe. Hieronder, in het algemeen deel van de toelichting, zal een zevental onderwerpen worden besproken, aansluitend bij de belangrijkste wijzigingsvoorstellen. Deze onderwerpen vertonen overigens niet noodzakelijkerwijs samenhang. Daarnaast bevat het wetsvoorstel nog een aantal aanpassingen – meest technische wijzigingen of verduidelijkingen – van de bij de eerste Wet computercriminaliteit ingevoerde bepalingen. Deze zullen in het artikelsgewijze deel van de toelichting kort worden toegelicht. Ik voorzie overigens dat in de naaste toekomst nieuwe onderwerpen regeling zullen behoeven, onder andere op grond van de hierna te bespreken internationale ontwikkelingen. Die onderwerpen zijn thans echter nog onvoldoende uitgekristalliseerd, zodat daarvoor nog geen voorziening kan worden getroffen. De belangrijkste voorstellen vallen uiteen in de volgende onderwerpen.

*De aansprakelijkheid van tussenpersonen (paragraaf 2)*

De opkomst van nieuwe tussenpersonen bij de openbaarmaking en verspreiding van informatie (bijvoorbeeld Internet Service Providers), in combinatie met bepaalde kenmerken van moderne informatietechnologie (snelheid, anonimiteit, internationalisering), vraagt om een nadere regeling van hun eventuele strafrechtelijke aansprakelijkheid ingeval zij betrokken zijn bij de verspreiding van strafbare informatie. Daartoe wordt een uitbreiding en modernisering van de thans tot uitgevers beperkte regeling van artikel 53 Sr voorgesteld, waarbij tussenpersonen uitgesloten worden van vervolging indien zij aan bepaalde voorwaarden voldoen.

*Vernietiging van computergegevens (paragraaf 3)*

Het Wetboek van Strafvordering regelt nu slechts het onderzoek naar en

de vastlegging van gegevens in geautomatiseerde werken met het oog op de waarheidsvinding. Niet is geregeld wat opsporingsambtenaren kunnen doen als zij gegevens aantreffen die onderwerp uitmaken van een strafbaar feit (een bestand met strafbare informatie) of met behulp waarvan een strafbaar feit is gepleegd (bijvoorbeeld een virusprogramma). Voorgesteld wordt daarom – analoog aan de regeling van de inbeslagneming en onttrekking aan het verkeer van voorwerpen – een mogelijkheid om computergegevens onder bepaalde voorwaarden bij wijze van voorlopige maatregel ontoegankelijk te maken en uiteindelijk door de rechter te doen vernietigen.

*Medewerking aan de ontsleuteling van gegevens (paragraaf 4)*

De versleuteling van gegevens opgeslagen in computers of overgedragen via telecommunicatie vormt in toenemende mate een probleem voor de bewijsgaring. Thans bestaat reeds in artikel 125k Sv de mogelijkheid om bij een huiszoeking bepaalde personen zoals de netwerkbeheerder te verplichten mee te werken aan de ontsleuteling van in de computers aangetroffen gegevens. Voorgesteld wordt deze medewerkingsverplichting door te trekken naar de telecommunicatie, zodat personen van wie redelijkewijs kan worden vermoed dat zij over die kennis beschikken, – binnen bepaalde grenzen – kunnen worden verplicht om om mee te werken aan het ontsleutelen van afgetapte gegevens.

*Het onderscheid tussen opgeslagen en stromende gegevens (paragraaf 5)*

Door technologische ontwikkelingen is het onderscheid tussen in een computer opgeslagen gegevens en gegevens die in een proces zijn van verwerking of overdracht tussen computers (stromende gegevens) niet steeds helder. Aangegeven wordt waarom dit onderscheid niettemin, met name uit een oogpunt van precieze omschrijving van strafbare feiten en strafvorderlijke bevoegdheden, noodzakelijk is. Met het oog op de rechtszekerheid worden een groot aantal terminologische verduidelijkingen voorgesteld.

*Onderzoek van e-mail (paragraaf 6)*

Voorgesteld wordt elektronische post in het strafrecht dezelfde mate van bescherming te geven als een brief of een telefoongesprek. Dit leidt tot een verruiming van de strafbaarstelling van werknemers van een telecommunicatieaanbieder die wederrechelijk kennisnemen van niet voor hen bestemde gegevens (thans artikel 374bis Sr) en een aanscherping van de eisen die worden gesteld aan het opsporingsonderzoek in de geautomatiseerde werken van telecommunicatieaanbieders.

*Opsporingsonderzoek op openbare computernetwerken (paragraaf 7)*

Kort wordt ingegaan op de positie van (Nederlandse) opsporingsambtenaren op openbare en grensoverschrijdende computernetwerken zoals Internet en enkele daarbij geldende uitgangspunten. Voorgesteld wordt een uitbreiding van de in de wet van 27 mei 1999 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden) (Stb. 245) voorziene pseudokoopbepaling tot het door een opsporingsambtenaar op bevel van de officier van justitie van een verdachte persoon afnemen van computergegevens door tussenkomst van een openbaar telecommunicatienetwerk.

*Overige wijzigingen (paragraaf 8)*

Behalve de reeds genoemde meer technische aanpassingen van de bij de Wet computercriminaliteit geïntroduceerde strafbepalingen bevat het wetsvoorstel ook enkele nieuwe strafbaarstellingen. In het bijzonder gaat het om de uitbreiding van de artikelen 350a en 350b Sr tot het wederrechtelijk veranderen, wissen enz. van *stromende* computergegevens en de strafbaarstelling van ernstige vormen van het zogenaamde *spammen.*

Een concept van dit wetsvoorstel is voor consultatie rondgezonden aan een aantal instanties. Adviezen zijn ontvangen van de Nederlandse Vereniging voor Rechtspraak (NVvR), de Nederlandse Orde van Advocaten (NOvA), het College van procureurs-generaal van het Openbaar Ministerie (OM), de Beleidsadviesgroep digitaal rechercheren (namens het Korpsbeheerdersberaad en de Raad van Hoofdcommissarissen tezamen), de Registratiekamer, de Vereniging van Nederlandse Internet Providers (NLIP), de Stuurgroep Informatietechnologie en Criminaliteit van het Platform Criminaliteitsbeheersing, de Nederlandse Orde van Register EDP-Auditors (NOREA) en de Juridische Commissie van de Federatie van Organisaties in het Bibliotheek-, Informatie- en Dokumentatiewezen (FOBID)[1]. Tot mijn tevredenheid zijn de adviezen over het geheel genomen op de hoofdpunten instemmend. Daarnaast bevatten ze een groot aantal opmerkingen en voorstellen, die op uiteenlopende onderdelen tot aanpassingen van het wetsvoorstel dan wel tot verduidelijking van de toelichting hebben geleid. Waar nodig zal ik in de toelichting op de adviezen ingaan.
Dit wetsvoorstel bevat géén voorzieningen op het terrein van het internationale strafrecht en de internationale rechtshulp. Aan dergelijke voorzieningen wordt inmiddels in internationaal verband gewerkt. Ik wijs met name op de werkzaamheden van het Committee of Experts on Crime in Cyber-space (PC-CY), dat door de Raad van Europa is ingesteld met als opdracht een veelomvattend internationaal verdrag ter zake van de bestrijding van grensoverschrijdende computercriminaliteit voor te bereiden. Daarin zullen zaken als verdeling van rechtsmacht en grensoverschrijdende netwerkzoekingen een regeling moeten vinden. Ik meen dat dit initiatief uitzicht biedt op een internationale oplossing van de problemen die op dit vlak bestaan, mede omdat ook landen als de Verenigde Staten en Canada, alsmede de UNESCO aan de beraadslagingen deelnemen. Daarnaast wijs ik erop dat, onder andere in EU-verband, hard wordt gewerkt aan afspraken over specifieke maatregelen ter bestrijding van kinderporno op Internet (zie mijn uitgebreide antwoord van 7 augustus 1998 op kamervragen, aanhangsel Handelingen II 1997/98, nr. 1644). In het toetsingskader van de Nota Wetgeving voor de elektronische snelweg wordt de noodzaak van internationale regelgeving – bij voorkeur op mondiaal niveau, eventueel in kleiner verband (Raad van Europa, Europese Unie) – duidelijk onderstreept. Dit laat echter onverlet dat, teneinde internationaal goed te kunnen samenwerken bij de aanpak van grensoverschrijdende computercriminaliteit, de nationale wetgeving van de samenwerkende partijen op orde en bij de tijd dient te zijn. Het onderhavige wetsvoorstel dient mede tegen deze achtergrond te worden bezien.

Tot slot vraag ik de aandacht voor twee ontwikkelingen in het verband van de Europese Unie die mogelijk nog gevolgen hebben voor het wetsvoorstel en de verdere gang daarvan.
Op 23 december 1998 heeft de Europese Commissie een voorstel voor een *richtlijn van het Europees Parlement en de Raad betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt* ingediend (PbEG C 30). In dit voorstel is onder andere een regeling van de aansprakelijkheid van tussenpersonen opgenomen, die blijkens de

[1] Ter inzage gelegd bij de afdeling Parlementaire Documentatie.

toelichting daarop ook bedoeld is te gelden voor het strafrecht. De door de Commissie voorgestelde aansprakelijkheidsregeling heeft een andere invalshoek en opzet dan de in artikel 53 Sr voorgestelde regeling. Waar artikel 53 Sr een algemene regeling geeft die voor alle tussenpersonen geldt, onderscheidt het voorstel van de Commissie drie typen activiteiten van tussenpersonen – waarbij het bovendien alleen gaat om elektronische diensten –, met daaraan vastgeknoopt drie verschillende aansprakelijkheidsregimes. Hoewel ik het toejuich dat de Europese Unie zich de juridische aspecten van Internet aantrekt, kleven mijns inziens aan de voorgestelde aansprakelijkheidsregeling enige bezwaren, nog daargelaten de prealabele vraag of de Commissie wel bevoegd is om in het kader van de interne markt regels te stellen met betrekking tot het strafrecht van de lidstaten. Het moge duidelijk zijn dat deze bezwaren tijdens de thans lopende onderhandelingen over het richtlijnvoorstel van Nederlandse zijde worden ingebracht, waarbij uiteraard wordt aangehaakt bij de uitgangspunten van de in dit wetsvoorstel neergelegde regeling. Zou niettemin het voorstel van de Europese Commissie in de huidige vorm tot richtlijn worden verheven, dan zou dit mogelijk tot wijziging van de in artikel 53 Sr voorgestelde aansprakelijkheidsregeling nopen.
De tweede ontwikkeling die van belang is, betreft een aanstaande uitbreiding van *Richtlijn 98/34/EG betreffende een informatieprocedure op het gebied van normen en technische voorschriften* (de zogenaamde notificatierichtlijn) tot voorschriften betreffende «diensten van de informatiemaatschappij» (zie voor de wijziging Richtlijn 98/48/EG, PbEG L 217). De implementatietermijn van deze richtlijn loopt op 5 augustus 1999 af, zodat de lidstaten vanaf dat moment de ontwerpen van dergelijke voorschriften bij de Commissie moeten aanmelden alvorens de nationale wetgevers die voorschriften in definitieve vorm mogen vaststellen. Na aanmelding dient een zogenaamde standstill-termijn van drie maanden in acht te worden genomen, gedurende welke de Commissie en de andere lidstaten het betrokken ontwerp-voorschrift op zijn verenigbaarheid met het Europese recht kunnen beoordelen. Het onderhavige wetsvoorstel bevat vermoedelijk voorschriften betreffende «diensten van de informatiemaatschappij», waaronder mogelijk het voorgestelde artikel 53 Sr. Aangezien in redelijkheid niet valt te verwachten dat het wetsvoorstel op 5 augustus a.s. door de Tweede Kamer zal zijn aangenomen, zal het wetsvoorstel waarschijnlijk dan moeten worden genotificeerd met inachtneming van de gebruikelijke standstill-periode. Hierover vindt thans overleg plaats met de Europese Commissie.
Bij deze wetgevingstechnisch gezien weinig gelukkige, maar in de gegeven omstandigheden onvermijdbare samenloop van nationale en Europese wetgevingsprocedures heb ik overwogen met de indiening van het wetsvoorstel te wachten totdat duidelijkheid bestaat over de gevolgen van het (komende) Europese recht voor het wetsvoorstel, in het bijzonder voor het voorgestelde artikel 53 Sr. Die duidelijkheid zal er echter waarschijnlijk niet voor het eind van 1999 zijn. Een dergelijk lange periode van stilstand – bovenop de toch al lange voorbereidingsduur van dit wetsvoorstel – leek mij onwenselijk, gelet op het belang van de materie en gelet op het feit dat het merendeel van de voorstellen in het geheel niet wordt geraakt door de bedoelde Europese ontwikkelingen. Ik heb dan ook besloten het wetsvoorstel thans reeds in te dienen, zodat de Tweede Kamer, zo zij dit wenst, met de behandeling een aanvang kan maken. Zodra er meer duidelijkheid is over de richting van de Europese besluitvorming en over de eventuele consequenties daarvan voor het onderhavige wetsvoorstel, zal ik de Kamer berichten. Indien gewenst ben ik uiteraard graag bereid met de Kamer te overleggen over de te volgen procedure.

## 2. De aansprakelijkheid van tussenpersonen

*2.1 Achtergrond*

De afgelopen jaren is maatschappelijke onrust ontstaan over de aanwezigheid op het internationale computernetwerk Internet van een grote hoeveelheid strafbaar materiaal, waarvan met name kinderporno de aandacht heeft getrokken. De kenmerken van Internet brengen mee dat dergelijk materiaal snel en op eenvoudige wijze wereldwijd verspreid kan worden en voor een groot publiek beschikbaar kan worden gemaakt, terwijl de afzenders of verdere verspreiders moeilijk traceerbaar zijn of niet grijpbaar voor nationale overheden omdat ze zich in het buitenland bevinden. De vraag komt op wat in dit geval de rol is van de zogenaamde Internet Service Providers (ISP's), de bedrijven die toegang verlenen tot Internet en daarbij specifieke diensten aanbieden zoals elektronische post *(e-mail)*, faciliteiten voor het maken van een openbare pagina op het *World Wide Web* (een *website)* en de toegang tot discussie- of nieuwsgroepen. Mijn ambtsvoorganger heeft zich bij verschillende gelegenheden op het standpunt gesteld dat de providers reeds naar huidig recht onder omstandigheden strafrechtelijk aansprakelijk zijn – te denken valt aan medeplichtigheid – voor de via hen verspreide strafbare informatie mits zij op de hoogte waren van de aard van de informatie, althans indien het aan hun ernstige nalatigheid te wijten was dat het betrokken materiaal op Internet voor het publiek beschikbaar was (zie het antwoord d.d. 19 augustus 1996 op kamervragen over strafbare informatie op de computer van de Technische Universiteit Eindhoven, kamerstukken II 1995/96, Aanh. 1582). Wel heeft zij bij die gelegenheden aangekondigd te zullen onderzoeken of de providers een speciale bescherming dienen te krijgen, net als thans in de artikelen 53 en 54 van het Wetboek van Strafrecht is voorzien voor uitgevers en drukkers, opdat zorgvuldig handelende providers niet bevreesd behoeven te zijn voor een strafvervolging.
Bij het bedoelde onderzoek is gebleken dat niet volstaan kan worden met een aanvullende bepaling voor de Internet Service Providers, maar dat een ingrijpende herziening van met name artikel 53 Sr gewenst is. Dit artikel, dat is ontstaan in een tijd waarin de drukpers nog het belangrijkste middel voor de publicatie van meningen en andere uitlatingen was, is ernstig verouderd als gevolg van de ontwikkelingen in deze eeuw op het terrein van de informatievoorziening: radio en televisie werden belangrijke media en kabel en satellieten vergemakkelijken het gegevensverkeer aanzienlijk. De laatste jaren zijn de ontwikkelingen onverminderd doorgegaan. Van een hulpmiddel bij de be- en verwerking van gegevens is de computer geworden tot een belangrijk communicatiemiddel. Dit is tevens illustratie van een andere ontwikkeling: de toenemende convergentie van traditioneel gescheiden media (radio, TV, telefoon, computer). Bij de grondwetsherziening van 1983 werd reeds rekening gehouden met deze en nog onvoorziene ontwikkelingen doordat de drukpersvrijheid werd uitgebreid tot de vrijheid om door radio, televisie of *enig ander middel* gedachten of gevoelens te openbaren, zonder voorafgaand toezicht op de inhoud daarvan (artikel 7, tweede en derde lid, Grondwet). Artikel 53 Sr dient dienovereenkomstig te worden uitgebreid.

*2.2 Uitings- en verspreidingsdelicten*

Voor het openbaren van gedachten of gevoelens heeft niemand voorafgaand verlof (wegens de inhoud daarvan) nodig «behoudens ieders verantwoordelijkheid volgens de wet» (artikel 7 Grondwet). De laatste clausule doelt met name op de (repressieve) aansprakelijkheid volgens de strafwet. Het Wetboek van Strafrecht kent verschillende bepalingen waarin het doen van bepaalde uitingen wordt strafbaar gesteld: klassieke strafbepalingen, zoals belediging van de Koning (artikel 111), opruiing

(artikel 131), smalende godslastering (artikel 147) en smaad (artikel 261), en bepalingen van meer recente datum, zoals die betreffende discriminatie (artikel 137c en 137d). Naast, en nauw verbonden met, deze uitingsdelicten kent het wetboek strafbaarstellingen die betrekking hebben op de verspreiding van geschriften, afbeeldingen of voorwerpen waarin een bepaalde strafbare uiting is vervat, en op gedragingen die op die verspreiding zijn gericht, zoals het in voorraad hebben van die geschriften en dergelijke (vgl. artikelen 113, 132 en 137e, tweede lid, onder 2, Sr). De vraag is of de omschrijving van deze uitings- en verspreidingsdelicten nog bij de tijd is en voldoende rekening houdt met moderne vormen van communicatie en informatievoorziening. Dat is naar ik meen het geval. Zo kan het via computernetwerken transporteren, kopiëren, ter beschikking stellen en oproepen van gegevens gevat worden onder begrippen als «verspreiden», «in voorraad hebben» of «tentoonstellen». Ook de term «geschrift» leent zich voor modernere toepassingen. Zo kunnen er ook lp's, cd's en videobanden onder worden begrepen, zoals blijkt uit de artikelen 113, tweede lid, 132, tweede lid, 147a, tweede lid, en 261, tweede lid, Sr, waar sprake is van het «ten gehore brengen» van de inhoud van een geschrift. Volgens prof. Remmelink valt er iedere mechanische reproductie van gedachten door het woord onder (Het Wetboek van Strafrecht, losbladig commentaar, aant. 5 op artikel 113). Zo verstaan omvat «geschrift» ook een door een computer opgeroepen en op het beeldscherm gebracht gegevensbestand. Hierbij moet worden aangetekend dat de weinige keren dat de Hoge Raad zich over een bestand moest uitlaten, wel de eis stelde van enigerlei duurzame vastlegging van dat bestand (vgl. HR 24 maart 1998, Nieuwsbrief Strafrecht 1998, 5, nr. 067, blz. 92, waarbij een elektronisch gedane belastingaangifte als een geschrift werd aangemerkt mede omdat zij gedurende enige jaren daarna raadpleegbaar bleef). De vraag is bijvoorbeeld of het tijdelijk opslaan van een bestand in het werkgeheugen van een computer een «geschrift» in strafrechtelijke zin kan opleveren. Vooralsnog kan op dit punt mijns inziens de rechtsontwikkeling worden afgewacht. Kortom: de huidige strafbepalingen behoeven nog geen aanpassing aan nieuwe informatietechnieken; ze zijn tot dusver voldoende «techniek-onafhankelijk». Een onderzoek in het kader van het Nationaal Programma van Informatietechnologie en Recht leidde tot dezelfde conclusie (Th. de Roos, G. Schuijt en L. Wissink, Smaad, laster, discriminatie en porno op het Internet, Alphen aan den Rijn/Diegem 1996).

Bijzonder kenmerk van de uitings- en verspreidingsdelicten is dat het desbetreffende handelen doorgaans alleen strafbaar is indien het openlijk, in het openbaar, althans met het oog op openbaarmaking, geschiedt. Wat in het privéverkeer tussen twee of meer personen plaatsheeft, is in de regel niet strafbaar. Integendeel, communicatie die gericht is op geheimhouding vormt een apart te beschermen belang (vgl. de «freedom of correspondence» van artikel 8 EVRM). Hoewel bij de huidige ontwikkelingen de grenzen tussen openbaar en privé, openbaar en besloten verschuiven en soms vervagen, is het nodig aan dit onderscheid vast te houden teneinde in voorkomend geval een juiste afweging tussen botsende grondrechten mogelijk te maken. Criterium voor strafbaarstelling dient te zijn of door bepaald handelen de openbare orde is geschaad, zij het wellicht op indirecte wijze. Wat nog besloten is en wat openbaar, dient uiteindelijk aan de interpretatie door de rechter te worden overgelaten. «Openbaar» wil volgens de gangbare opvatting zeggen: ten overstaan van het publiek, algemeen toegankelijk, onverschillig of de toegankelijkheid aan enige voorwaarde of betaling van entree is gebonden (Het Wetboek van Strafrecht, a.w., aant. 4 op artikel 131). In deze zin is bijvoorbeeld veel van de communicatie op Internet, met zijn miljoenen en eenvoudig tot stand te brengen aansluitingen, zeker openbaar (de meeste nieuwsgroepen en websites). Het verzenden van een e-mail aan een bepaalde persoon (of aan een bepaalde, welomschreven

groep van personen die als besloten kan worden aangemerkt), daarentegen, zal als privé moeten worden aangemerkt, net als het versturen van een «echte» brief. Hetzelfde geldt voor bepaalde chatboxen waarin personen, als ware het per telefoon, met elkaar kunnen communiceren. Aparte vermelding verdient in dit verband artikel 240b Sr, strafbaarstellende het verspreiden, openlijk tentoonstellen, voorhanden hebben enz. van kinderporno. Door een recente uitspraak van de Hoge Raad is op het punt van het voorhanden hebben aan dit delict het openbare karakter (althans de externe connotatie) komen te ontvallen. De Hoge Raad maakte namelijk uit dat het in bezit hebben van kinderporno voor eigen gebruik (eventueel zelfs het bezit van een enkele afbeelding) «in voorraad hebben» in de zin van artikel 240b Sr kan opleveren (HR 21 april 1998, NJB 1998, blz. 1005, nr. 81).

*2.3 De huidige regeling van de uitgeversaansprakelijkheid*

Voor uitgevers en drukkers achtte de wetgever van 1881 een afwijking noodzakelijk van de normale regels van strafrechtelijke aansprakelijkheid voor delicten als belediging en opruiing gepleegd door middel van de drukpers.[1] Waar de Grondwet censuur vanwege de staat verbood, moest worden voorkomen dat uitgevers en drukkers zich gedwongen zouden voelen om in plaats van die staat zelf censuur uit te oefenen op hetgeen zij uitgaven c.q. drukten. Dit gevaar van zelfcensuur werd aanwezig geacht omdat uitgevers en drukkers zich in de normale uitoefening van hun beroep schuldig zouden kunnen maken aan medeplichtigheid of medeplegen wanneer zij een geschrift met een strafbare inhoud uitgaven of drukten. Voor dat geval werden de artikelen 53 en 54 in het wetboek opgenomen, die hen van vervolging vrijwaarden mits zij een bepaalde zorgvuldigheid in acht namen: de uitgever of drukker moest op het betrokken stuk zijn naam en woonplaats vermelden en hij moest de dader – in het geval van de drukker: degene op wiens last het stuk is gedrukt –, dat wil zeggen degene van wie het strafbare stuk afkomstig was, bekendmaken (als die nog niet bekend was). Voldeed de uitgever of drukker niet aan deze voorwaarden, dan genoot hij niet de bescherming van de artikelen 53 of 54 en waren op hem de normale regels van strafrechtelijke aansprakelijkheid van toepassing. Hetzelfde gold wanneer de uitgever of drukker in zee ging met iemand die niet «grijpbaar» was voor justitie omdat hij niet vervolgbaar was of buiten het rijk in Europa woonde. In dat geval droeg de uitgever of drukker er aan bij dat de aansprakelijke persoon buiten de handen van justitie bleef en kon hij niet terugvallen op artikel 53 of 54. Bij dit alles dient te worden aangetekend dat de uitgever en drukker – onder de genoemde voorwaarden – alleen van vervolging werden gevrijwaard indien zij zich beperkten tot hun normale arbeid, hetgeen tot uitdrukking werd gebracht door de woorden «wordt de uitgever *als zoodanig* niet vervolgd». Wie geschriften met een strafbare inhoud uitgaf of drukte die hij zelf had geschreven of tot het schrijven waarvan hij een ander had uitgelokt, verdiende geen bijzondere bescherming als uitgever of drukker.
Strijdpunt in de Tweede Kamer was in hoeverre de uitgever of drukker voor de inhoud van het betrokken stuk kon worden gestraft indien de voorwaarden van artikel 53 of 54 niet waren vervuld. Een deel – en met hen minister Modderman – vond dat de uitgever en drukker alleen volgens de normale regels als medeplichtige of medepleger konden worden gestraft. Dit betekende doorgaans dat bewezen moest worden dat zij kennis hadden gehad van de inhoud van het geschrift. Anders zou niet voldaan zijn aan het bestanddeel «opzettelijk» zoals dit voorkomt bij medeplichtigheid en de meeste uitingsdelicten. Volgens een ander deel van de Kamer daarentegen zou dit neerkomen op een vrijbrief voor de uitgever en drukker om alles uit te geven of te drukken, mits zij er geen kennis van namen. Als compromis zijn uiteindelijk de artikelen 418 en 419

[1] Zie voor de wetsgeschiedenis van de artikelen 53 en 54 Sr H.J. Smidt, Geschiedenis van het Wetboek van Strafrecht, eerste deel, Haarlem 1881, blz. 422 e.v.

ontstaan, die strafbaar stellen het uitgeven c.q. drukken van een geschrift of afbeelding van strafbare aard terwijl niet aan de voorwaarden van artikel 53 of 54 is voldaan (dat wil zeggen indien de dader noch bekend is noch op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, is bekendgemaakt, of indien de uitgever of drukker wist of moest verwachten dat de dader (of persoon op wiens last het stuk is gedrukt) op het tijdstip van de uitgave niet vervolgbaar of buiten het Rijk in Europa gevestigd zou zijn). In dat geval is de aansprakelijkheid van de uitgever of drukker, die als een aansprakelijkheid sui generis werd beschouwd, gegrond op onvoldoende voorzichtigheid bij het uitgeven of drukken.
Zoals gezegd is met name artikel 53 Sr, anders dan de uitings- en verspreidingsdelicten, niet meer bij de tijd. Ik wijs op de volgende punten.

– De klassieke drukpers is al lang niet meer het enige middel voor de openbaarmaking en verspreiding van uitingen. Radio, TV en computernetwerken zijn erbij gekomen. Tegelijkertijd vervagen de grenzen tussen deze middelen.
– Naast uitgevers zijn nieuwe bedrijven ontstaan met een vergelijkbare, intermediaire functie in de informatiemaatschappij. Denk aan kabelbedrijven en Internetproviders. En ook hier vervagen de grenzen (vgl. grote uitgevers die *on line* gaan).
– De wetgever van 1881 dacht bij drukpersdelicten aan de primaire openbaarmaking met behulp van de drukpers. Dáárin school het gevaar van (zelf-)censuur en niet in de verdere verspreiding van het gedrukte. Distributeurs zoals boekhandels verdienden dus geen bijzondere bescherming (H.J. Smidt, a.w., tweede deel, blz. 44–48). Deze opvatting is in de huidige informatiemaatschappij niet meer houdbaar: zij doet geen recht aan het grote belang van de verspreiding van informatie en de daartoe beschikbare middelen en miskent dat het onderscheid tussen drukken, uitgeven en verspreiden vervaagt.

*2.4 De voorgestelde regeling*

Ik meen dat het wenselijk is artikel 53 Sr op de genoemde punten aan te passen en te moderniseren. Ik noem daarvoor een aantal redenen: ten eerste het grote belang van een onbelemmerde informatievoorziening in een democratische rechtsstaat, voorts de verantwoordelijkheid voor de overheid om de vrijheid van de burger om door enig middel gedachten of gevoelens te openbaren te waarborgen en te bevorderen, en tot slot de steeds belangrijker wordende rol van personen die een intermediaire functie vervullen in de informatiemaatschappij. Zo veel mogelijk dient te worden voorkomen dat deze tussenpersonen zich gedwongen voelen tot een vorm van zelfcensuur. Dit neemt overigens niet weg dat zij een zekere verantwoordelijkheid hebben voor wat zij doorgeven, namelijk voor zover de betrokken informatie voor het publiek toegankelijk wordt gemaakt, en dat derhalve van hen een bepaalde zorgvuldigheid kan worden geëist. Nemen zij die zorgvuldigheid niet in acht, bijvoorbeeld door een anoniem geschrift van strafbare aard te verspreiden waarvan zij de aard kennen, dan moeten zij voor de strafrechter ter verantwoording kunnen worden geroepen. Beide aspecten – bescherming tegen vervolging van de tussenpersoon die normaal zijn beroep uitoefent, en aansprakelijkheid indien niet een zekere zorgvuldigheid in acht wordt genomen – dienen in een moderne regeling van de uitgeversaansprakelijkheid tot uitdrukking te worden gebracht.
De vraag zou kunnen worden gesteld of de bedoelde tussenpersonen – ook de nieuwe tussenpersonen zoals Internetproviders – niet reeds onder het wettelijke begrip «uitgever» kunnen worden begrepen, zodat wijziging van artikel 53 Sr mogelijk achterwege zou kunnen blijven. Daartoe zou een extensieve interpretatie nodig zijn. Hoewel niet ondenkbaar is dat de rechtspraak een dergelijke interpretatie zou willen aanvaarden, ben ik van

mening dat uit een oogpunt van rechtszekerheid een nieuwe wettelijke regeling, aangepast aan de moderne tijd, de voorkeur verdient. Ik word hierin gesteund door het reeds aangehaalde onderzoek van De Roos c.s. (Smaad, laster, discriminatie en porno op het Internet, a.w., blz. 200). Een wettelijke regeling waarin de grenzen van de strafrechtelijke aansprakelijkheid van tussenpersonen worden aangegeven, geeft duidelijkheid aan deze tussenpersonen. Zij laat overigens onverlet dat tussenpersonen kunnen overgaan tot enigerlei vorm van zelfregulering (vgl. het Meldpunt kinderporno van de Internet Service Providers). Wettelijke regeling zoals hier voorgesteld biedt juist ondersteuning voor dergelijke zelfregulering. Voor het belang en de mogelijkheden van zelfregulering op de elektronische snelweg verwijs ik naar de Nota Wetgeving voor de elektronische snelweg.

In de voorgestelde regeling wordt de uitgever in artikel 53 Sr vervangen door de professionele «tussenpersoon» die door enig middel (drukpers, computernetwerk) informatie afkomstig van derden beschikbaar maakt voor het publiek. Doel van deze wijziging is deze tussenpersoon als zodanig te vrijwaren van vervolging wegens zijn betrokkenheid bij uitings- of verspreidingsdelicten, mits voldaan is aan de in artikel 53 neergelegde voorwaarden. Is niet aan een van die voorwaarden voldaan, dan kan hij volgens de gewone regels die gelden voor daderschap en deelneming, worden gestraft en voorts wegens de overtreding van artikel 418 Sr, dat daartoe ook zal worden aangepast. Voorts is hij gewoon aansprakelijk voor eigenhandig gepleegde uitingsdelicten, waarbij hij niet in zijn hoedanigheid van tussenpersoon optreedt.

De nieuwe regeling van artikel 53 biedt tussenpersonen niet slechts bescherming bij het gebruik van de klassieke drukpers, maar ook bij het gebruik van «enig ander middel voor de openbaarmaking of verspreiding» van informatie («uitingen in woord, beeld of geluid»). Deze omschrijving omvat ook de modernere media, zoals radio en TV en, van recente datum, computernetwerken. Voor het begrip «tussenpersoon» is gezocht naar een algemene omschrijving van de functie van uitgever in de moderne informatiemaatschappij: een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in woord, beeld of geluid afkomstig van derden.[2] Hieronder vallen de (klassieke) uitgever, exploitanten van bioscopen, Internet-providers, boekhandels en bibliotheken. Dit is geen limitatieve opsomming. Het begrip «tussenpersoon» is een open begrip dat ook toekomstige personen of bedrijven kan omvatten met thans nog niet bestaande functies in de informatiemaatschappij. Aldus biedt het voorgestelde artikel 53 Sr mijns inziens een mooi voorbeeld van zogenaamde technologie-onafhankelijke regelgeving, die bestand is tegen de tand des tijds. De Nota Wetgeving voor de elektronische snelweg spreekt een duidelijke voorkeur uit voor technologie-onafhankelijke regelgeving.

Ik wijs erop dat de voorgestelde omschrijving van «tussenpersoon» niet alleen omvat personen die (beroeps- of bedrijfsmatig) informatie openbaar maken, maar ook degenen die die informatie (verder) verspreiden. Hieronder vallen ook reeds lang bestaande distributeurs, zoals bioscoopexploitanten of boekhandelaren, die tot nu toe geen bescherming onder de artikelen 53 of 54 Sr genoten. Er zijn verschillende redenen die rechtvaardigen dat zij die bescherming thans wel krijgen. Ten eerste wijs ik nog eens op de steeds belangrijkere rol die distributeurs zijn gaan spelen in de informatiemaatschappij met haar enorme aanbod van informatie en informatiemedia. Ten tweede kan worden vastgesteld dat vooral onder invloed van technologische ontwikkelingen (vgl. het Internet) de grens tussen de (primaire) openbaarmaking van informatie en de (verdere) verspreiding daarvan vervaagt, waardoor het moeilijker wordt de rechtsregimes die op het een en op het ander van toepassing zijn te onderscheiden. Tot slot merk ik op dat een beperking van het begrip «tussenpersoon» tot moderne distributeurs zoals Internet Service

[2] Van Dale omschrijft de uitgever als: «persoon die zich beroepshalve belast met het laten drukken of anderszins vermenigvuldigen van geschriften, om die aan het publiek te verkopen».

Providers en andere on-line-diensten tot het onwenselijke resultaat zou leiden dat een traditionele distributeur zoals een boekhandel die zou besluiten zijn diensten ook op Internet aan te bieden, in dat geval meer bescherming zou genieten dan bij zijn normale dienstverlening *off line.* Vooralsnog stel ik voor het voor de drukker geldende artikel 54 Sr te handhaven. Voor zover iemand zich beperkt tot het eigenlijke drukkerswerk – het verveelvoudigen van een geschrift met het oog op publicatie en verspreiding – en niet zelf de gedrukte werken openbaar maakt of verspreidt, valt hij niet onder het begrip tussenpersoon en is artikel 53 Sr dus niet op hem van toepassing. De reden waarom de drukker in 1881, naast de uitgever, een bijzondere bescherming kreeg – het zo veel mogelijk voorkomen van zelfcensuur bij een essentieel onderdeel van het publicatieproces –, is echter ook thans nog aanwezig en vormt nog steeds voldoende rechtvaardiging voor een aparte regeling. Tegelijk zijn de ontwikkelingen die de positie van bijvoorbeeld de uitgever ingrijpend hebben gewijzigd – de vervaging van het onderscheid tussen uitgeven en verspreiden in combinatie met het ontstaan van grens-overschrijdende, razendsnelle communicatiemedia, waardoor bijzondere handhavingsproblemen ontstaan – in veel mindere mate op de klassieke drukker van toepassing, zodat de regeling van artikel 54 Sr geen dringende aanpassing behoeft. Niet ondenkbaar is overigens dat op termijn het praktisch belang van een aparte regeling voor drukkers zo gering wordt, dat zij kan worden geschrapt.
De drie voorwaarden voor uitsluiting van vervolging van de tussen-persoon komen als volgt te luiden. Zij gelden cumulatief.

*a. Vereist is dat de tussenpersoon bij de openbaarmaking of verspreiding zijn identiteit heeft bekendgemaakt dan wel gegevens heeft verstrekt waardoor zijn identiteit kan worden achterhaald.*
Het huidige artikel 53 lid 1 Sr schrijft voor dat het gedrukte stuk de naam en woonplaats van de uitgever vermeldt. Bij moderne vormen van openbaarmaking of verspreiding zal het niet altijd mogelijk of gebruikelijk zijn om naam en woonplaats expliciet te vermelden. De Vereniging van Nederlandse Internet Providers (NLIP) heeft er in haar commentaar op het wetsontwerp op gewezen dat vermelding van de naam van de provider op een website op Internet niet functioneel is en mogelijk ongewenste neveneffecten voor de markt heeft. Daarom is in het voorliggende voorstel als alternatieve mogelijkheid opgenomen dat de tussenpersoon tegelijk met de openbaarmaking of verspreiding gegevens verstrekt waardoor zijn identiteit kan worden achterhaald. Waar het om gaat is dat die gegevens politie en justitie in staat stellen om – zonder onevenredige inspanning – langs andere weg de naam en woonplaats van de tussen-persoon te achterhalen. Bij Internet zal dit in het algemeen geen probleem zijn omdat met behulp van automatisch op ieder Internetbericht vermelde gegevens, zoals het adres van de afzender of de route die het bericht is gegaan, via de zogenaamde domain-registry (de beheerder van alle Internetadressen) kan worden achterhaald wie de tussenpersoon of tussenpersonen zijn en wat hun adres is.

*b. Vereist is dat de dader bekend is dan wel dat de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooron-derzoek is overgegaan, alle aanwijzingen heeft gegeven die redelijkerwijs van hem kunnen worden gevergd teneinde de dader te achterhalen.*
Strafrechtelijke vervolging van de tussenpersoon is geen doel op zich. Uiteraard dient het strafrechtelijk onderzoek primair te zijn gericht op de opsporing van de (hoofd)dader. Als de dader niet bekend is vereist artikel 53 thans dat de uitgever hem op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, bekendmaakt, of, zoals het voorgestelde artikel 53, eerste lid, onder b stelt, dat de tussenpersoon alle aanwijzingen geeft die redelijkerwijs van hem kunnen

worden gevergd teneinde de dader te achterhalen. Met «dader» wordt bedoeld degene die de strafbare uiting heeft gedaan of een belangrijk aandeel daarin of in de openbaarmaking of verspreiding ervan heeft gehad. Artikel 53, eerste lid, onder b, legt de tussenpersoon geen resultaatsverplichting op in de zin dat als met zijn aanwijzingen de dader niet zou kunnen worden gevonden, de tussenpersoon steeds aansprakelijk zou zijn. Er is sprake van een (geobjectiveerde) inspanningsverplichting: de tussenpersoon dient zich in te spannen om justitie het spoor naar de dader te wijzen. De tussenpersoon die zich dit bij voorbaat onmogelijk maakt door anonieme berichten door te geven waarvan de bron op geen enkele wijze te traceren is, voldoet niet aan deze verplichting. Hij neemt dus het risico op zich strafrechtelijk aansprakelijk te worden gesteld voor de eventuele strafbare inhoud van die berichten.
Aanvankelijk was de bestaande formulering (dat de tussenpersoon de dader moet bekendmaken) gehandhaafd. In de commentaren zijn hiertegen twee bezwaren geuit. Ten eerste heeft de NLIP erop gewezen dat op Internet voor de ISP nooit ondubbelzinnig is te bepalen wie de dader is. De provider kan slechts aangeven door middel van wiens account/password-combinatie de strafbare uiting is geplaatst. Deze combinatie kan echter door onbekenden zijn gestolen of gekraakt. Deze personen kunnen vervolgens dus via de website of het e-mail-adres van een ander strafbare informatie verspreiden. Verder is het tegenwoordig mogelijk om betrekkelijk anoniem e-mails te verzenden door ze niet rechtstreeks vanaf de (niet-anonieme) account bij de lokale provider te versturen maar via gratis verstrekte e-mailaccounts die zich op een server elders bevinden. De bedrijven die deze accounts verstrekken controleren doorgaans namelijk niet de door de aanvrager verstrekte identiteits-gegevens. Ook de Nederlandse Orde van Advocaten heeft de vrees geuit dat hier een te vergaande eis aan ISP's wordt gesteld, die er feitelijk toe zal leiden dat zij zelden een beroep op artikel 53 hebben. Ik meen dat deze vrees onder de thans voorgestelde formulering niet bewaarheid zal worden. Van de ISP wordt niet meer – maar ook niet minder – gevergd dan dat hij het spoor terugvolgt zover als dat redelijkerwijs binnen zijn (technische) mogelijkheden ligt. Dit betekent dat hij in ieder geval moet opgeven de bedoelde account/password-combinatie en de server die het laatst in de keten het bericht heeft doorgegeven. Voorgaande schakels behoeft hij slechts te noemen voor zover hij die met de hem ter beschikking staande technieken en zonder onevenredige inspanning kan achterhalen. Ook is het níet zo dat uit de eis van het geven van aanwijzingen met betrekking tot de dader volgt dat tussenpersonen verplicht zijn de identiteit van degene wiens informatie ze doorgeven, te verifiëren. Het voorgestelde artikel 53, eerste lid, onder a, creëert geen identificatieplicht. Wel is het zo dat de aan justitie te geven aanwijzingen betrouwbaar en verifieerbaar moeten zijn (het noemen van «Donald Duck» als dader is onvoldoende). Of de betrokken tussenpersoon aanwijzingen heeft gegeven die hem kunnen vrijwaren van vervolging, staat uiteindelijk ter beoordeling van de rechter, die daarbij rekening zal houden met hetgeen in de gegeven omstandigheden redelijkerwijs van de tussenpersoon kan worden gevergd.
Het tweede bezwaar is onder andere verwoord door de Stuurgroep Informatietechnologie en Criminaliteit van het Nationaal Platform Criminaliteitsbeheersing en door de Registratiekamer. Het heeft wederom met name betrekking op de openbaarmaking en verspreiding van strafbare informatie via Internet. Ten aanzien daarvan is het namelijk zo dat de door de Internet Service Providers te geven aanwijzingen doorgaans zullen bestaan uit de gegevens die automatisch door het Internetprotocol worden gegenereerd en toegevoegd aan een bepaald bericht en die de herkomst, bestemming en routering van dat bericht aangeven. Volgens de Stuurgroep Informatietechnologie en Criminaliteit volgt uit de voorwaarde dat de tussenpersoon de dader bekendmaakt, dat

ISP's de bedoelde herkomstgegevens standaard gedurende enige tijd ten behoeve van justitie moeten bewaren. De Registratiekamer is bevreesd voor een dergelijke uitleg en wijst op de onwenselijkheid dat ISP's standaard alle handelingen van hun abonnees zouden gaan «loggen». Met dit laatste ben ik het geheel eens. Het is in strijd met het privacyrecht om gegevens omtrent personen, waartoe de herkomstgegevens van een door een persoon verzonden bericht zeker behoren, langer te bewaren dan nodig is voor een redelijk eigen doel. Het systematisch bewaren en verzamelen van gegevens ten behoeve van de politie of justitie voor het eventuele geval dat die later nodig mochten blijken voor de opsporing van een strafbaar feit, is niet geoorloofd. Feitelijk zal dit doorgaans betekenen dat een ISP slechts aanwijzingen kan geven als bedoeld in artikel 53 lid 1 onder b Sr zolang de openbaarmaking of verspreiding duurt. Zodra de betrokken pagina's of berichten van het net zijn verdwenen, zijn ook de herkomstgegevens die naar de dader kunnen leiden, niet meer aanwezig. De ISP is, zoals gezegd, rechtens niet bevoegd ze te bewaren. Wanneer justitie later toch bij hem mocht aankloppen met een verzoek om aanwijzingen die kunnen helpen bij het achterhalen van de dader van een strafbaar feit, kan hem uiteraard moeilijk worden tegengeworpen dat hij niet meer over die gegevens beschikt. Anders gezegd: het kan redelijkerwijs niet van de tussenpersoon worden gevergd dat hij gegevens verstrekt die hij niet meer heeft omdat hij niet bevoegd was ze nog langer te bewaren. Mits hij alle andere aanwijzingen geeft die redelijkerwijs van hem kunnen worden gevergd en mits is voldaan aan de overige voorwaarden van artikel 53 Sr, kan hij zich dan toch op de bescherming van die bepaling beroepen.
Dit ligt anders wanneer justitie *nog terwijl de verspreiding aan de gang is,* de provider maant aanwijzingen te geven omtrent de bron, en de provider meldt vervolgens geen aanwijzingen te kunnen geven omdat de herkomstgegevens van het betrokken bericht zijn gewist (door de provider zelf of door een vorige schakel in de verspreiding). De ISP die berichten doorgeeft waarvan de herkomstgegevens zijn gewist of waarmee anderszins duidelijk kenbaar is geknoeid met als doel de herkomst te verbergen, kan geen aanspraak maken op de bescherming van artikel 53. Hij brengt zichzelf in de positie dat hij niet kan voldoen aan artikel 53, eerste lid, onder b, en laadt het risico op zich dat hij wordt vervolgd voor eventuele strafbare informatie die via hem is verspreid.

*c. Vereist is dat de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle handelingen heeft verricht die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van verdere verspreiding.*
Artikel 53 Sr kent thans nog een derde voorwaarde, die betrekking heeft op de «grijpbaarheid» van de (hoofd)dader van het uitingsdelict. Deze voorwaarde houdt in dat de dader ten tijde van de uitgave binnen het Rijk in Europa gevestigd was. Deze voorwaarde stamt uit een tijd dat van grensoverschrijdende strafbare feiten – althans op het onderhavige terrein – weinig sprake was. Zat de dader – bij uitzondering – wel in het buitenland, dan achtte men het gerechtvaardigd terug te «grijpen» op de uitgever. Bij de huidige internationalisering van het (informatie)verkeer, waarbij auteurs en verspreiders vaak in verschillende landen zijn gevestigd, zou handhaving van de op genoemde wijze geformuleerde voorwaarde de reikwijdte van de vervolgingsuitsluitingsgrond voor tussenpersonen onaanvaardbaar beperken. Dit geldt met name voor tussenpersonen op een wereldomspannend netwerk als Internet. Zij zouden slechts zelden een beroep op artikel 53 hebben. Voorts is het zo dat in toenemende mate via rechtshulp- en uitleveringsverdragen instrumenten ter beschikking komen waardoor geciviliseerde staten in goede samenwerking en op een adequate wijze internationale criminaliteit kunnen aanpakken, zodat van staten mag worden verwacht dat ze deze

instrumenten gebruiken – en verder ontwikkelen – om de (hoofd)dader te kunnen vervolgen.
Het is dus zaak de verantwoordelijkheid van tussenpersonen op andere wijze vorm te geven, onafhankelijk van de rechtsmacht en de feitelijke mogelijkheden die Nederland heeft met betrekking tot de vervolging van de dader. De oplossing die is gekozen, knoopt aan bij de mogelijkheden die de (zich hier te lande bevindende) tussenpersoon heeft om een einde te maken aan de strafbare verspreiding van bepaalde uitingen. Daartoe wordt de derde voorwaarde van artikel 53 aldus geformuleerd dat «de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle handelingen heeft verricht die redelijkerwijs van hem kunnen worden gevergd ter voorkoming van verdere verspreiding.» Deze voorwaarde kan, afhankelijk van de omstandigheden en de stand van de techniek, meebrengen dat de tussenpersoon in contact treedt met de klant die via hem strafbare uitingen verspreidt, en zo nodig stappen tegen deze onderneemt, of dat de tussenpersoon de technische maatregelen neemt om een einde te maken aan de verspreiding. Een voorbeeld van dit laatste is dat een Internet Service Provider besluit om een bepaalde nieuwsgroep (waarin bijvoorbeeld kinderporno wordt uitgewisseld) niet meer aan zijn abonnees door te geven. De tussenpersoon behoeft niet zelf het initiatief te nemen om maatregelen te treffen, maar kan wachten totdat hij daartoe door de officier van justitie die een gerechtelijk vooronderzoek heeft gevorderd, wordt gemaand. De noodzaak tot het treffen van maatregelen tegen de verspreiding van strafbaar materiaal staat primair ter beoordeling van de officier van justitie, evenals de vraag wat precies van de tussenpersoon kan worden gevergd. Dit laatste zal van geval tot geval, mede afhankelijk van de stand van de techniek, moeten worden beoordeeld. Bij de afweging welke maatregelen redelijkerwijs van de tussenpersoon kunnen worden gevergd, dient de officier van justitie de eisen van proportionaliteit en subsidiariteit goed in het oog te houden. Een al te rigoureuze invulling van de voorwaarde van artikel 53, eerste lid, onder c, Sr zou immers de neiging tot zelfcensuur van tussenpersonen kunnen aanwakkeren, terwijl een van de doelstellingen van artikel 53 nu juist is om dat zoveel mogelijk te voorkomen. Bij zijn invulling van de onderhavige voorwaarde staat de officier van justitie onder controle van de rechter: in eerste instantie de rechter-commissaris en eventueel, als de officier van justitie toch tot vervolging overgaat, de zittingsrechter.

Tot slot zij benadrukt dat artikel 53 de aansprakelijkheid volgens de strafwet niet uitbreidt maar juist beperkt. Met het nieuwe begrip «tussenpersoon» is dan ook geenszins beoogd meer personen onder het bereik van de strafwet te brengen dan tot nu toe het geval is. Integendeel, anders dan voorheen profiteren bijvoorbeeld ook boekhandelaren en bioscoopexploitanten van de vervolgingsuitsluitingsgrond. Voorts is het zo dat de eisen die gelden voor daderschap en deelneming, onverkort op de tussenpersonen van toepassing zijn. Niet gerechtvaardigd is dan ook de vrees, die hier en daar wel doorklinkt, dat voortaan ook personen of bedrijven strafrechtelijk aansprakelijk zouden kunnen worden gesteld die louter als «doorgeefluik» voor uitingen fungeren en niet over de (technische) mogelijkheden beschikken om aan die uitingen een einde te maken. In zo'n geval zal van daderschap of medeplichtigheid geen sprake zijn. Daarvoor is immers een zekere beschikkingsmacht of macht tot ingrijpen vereist. Ik wijs ook op de criteria van het IJzerdraad-arrest (HR 23 februari 1954, NJ 1954, 378), die gelden voor functioneel daderschap: vermocht betrokkene erover te beschikken en placht hij te aanvaarden dat de litigieuze handelingen plaatsvonden? Zij die slechts de technische middelen verschaffen die noodzakelijk zijn voor de overdracht van of toegang tot bepaalde informatie zònder reële mogelijkheid tot ingrijpen, zullen in het algemeen dus niet als tussenpersoon aansprakelijk kunnen

worden gesteld. Dit zal bijvoorbeeld gelden voor een bibliotheek voor zover deze voor haar bezoekers terminals ter beschikking heeft die verbonden zijn met Internet; welke informatie die bezoekers raadplegen valt buiten haar beschikkingsmacht (bij het uitlenen van boeken met een strafbare inhoud ligt dit uiteraard anders). Van daderschap zal evenmin sprake zijn bij kabelexploitanten voor zover dezen een wettelijke doorgifteplicht hebben (vgl. artikel 82i Mediawet): wie rechtens zonder meer gehouden is bepaalde informatie door te geven, kan niet geacht worden die informatie te «verspreiden» of «openbaar te maken» (een beroep op overmacht is in dit soort gevallen ook denkbaar).
De Registratiekamer heeft gevraagd om een nadere verheldering welk handelen of nalaten van een Internet Service Provider hem tot dader of medeplichtige maakt. Volstrekte helderheid valt hierover echter niet te geven. Daderschap en termen als «verspreiden» en «openbaarmaken» zijn dynamische begrippen, die steeds opnieuw, in een veranderende omgeving, hun invulling moeten krijgen, mede gelet op de maatschappelijke eisen en verwachtingen. De rechtspraak zal derhalve moeten worden afgewacht. Daarbij gaat het zoals gezegd onder andere om de vraag in hoeverre de ISP in staat is in te grijpen in de verspreiding en verondersteld mag worden met de verspreiding in te stemmen. In zijn algemeenheid meen ik dat het aan de eigen abonnees ter beschikking stellen van computerruimte voor het openbaar maken van een website grond kan zijn voor het aannemen van daderschap of medeplichtigheid van de ISP. Ditzelfde geldt waarschijnlijk voor het aanbieden van een zogenaamde cache-service (een faciliteit waardoor informatie die door abonnees veelvuldig van buitenlandse servers wordt opgevraagd, tijdelijk op de server van de ISP wordt opgeslagen). Of het aanbrengen van een zogenaamde hyperlink (een verwijzing op een website naar bepaalde (bijvoorbeeld strafbare) informatie op een andere site) moet worden aangemerkt als het «verspreiden» van die informatie, kan ik in zijn algemeenheid niet met enige zekerheid zeggen, laat staan of de ISP van degene die de hyperlink aanbrengt, daaraan medeplichtig kan worden geacht.
Tot slot wijs ik erop dat waar werknemers van tussenpersonen de gelegenheid die hun functie hun biedt gebruiken om eigenhandig strafbare informatie te verspreiden, geen sprake is van een «als zodanig» handelende tussenpersoon en artikel 53 Sr dus niet van toepassing is. Of de tussenpersoon (dat wil zeggen de werkgever) eventueel zelf strafrechtelijk aansprakelijk kan worden gesteld voor het handelen van de werknemer, hangt af van de vraag of hij als functioneel dader kan worden aangemerkt. Dit is bij een werknemer die volstrekt buiten zijn boekje gaat, twijfelachtig.

*2.5 De aansprakelijkheid van de tussenpersoon; verwijtbaarheid*

De keerzijde van de bescherming van de tussenpersoon op grond van artikel 53 Sr is dat deze persoon onder omstandigheden strafrechtelijk aansprakelijk is voor zijn rol bij een uitings- of verspreidingsdelict dan wel als dader van artikel 418 Sr. Het niet voldoen aan een of meer van de voorwaarden van artikel 53 leidt op zichzelf echter nog niet tot aansprakelijkheid van de tussenpersoon. Artikel 53 ziet namelijk op de *vervolg*baarheid van een bepaalde persoon. Daarna komt nog de vraag of het telastegelegde feit kan worden bewezen, of het een strafbaar feit oplevert en of de verdachte daarvoor strafbaar is (vgl. de artikelen 348 en 350 Sv). Aan het slot van de vorige paragraaf is reeds iets gezegd over het vereiste daderschap. Als dat er niet is (of medeplichtigheid), zal de telastegelegde gedraging vermoedelijk niet bewezen kunnen worden. Daarnaast is, in verband met de strafbaarheid van de tussenpersoon, met name de vraag naar de verwijtbaarheid van belang: ingevolge het strafrechtelijke schuldbeginsel kan een persoon pas dan schuldig worden verklaard aan een strafbaar feit, als dat feit hem kan worden verweten. Voor de goede

orde wijs ik erop dat de vraag naar de vervolgbaarheid van de tussenpersoon en die naar diens strafbaarheid weliswaar zijn te onderscheiden, maar niet los van elkaar kunnen worden gezien. Artikel 53 Sr loopt namelijk vooruit op de vraag naar de strafbaarheid: het veronderstelt dat sprake is van een strafbare betrokkenheid van de tussenpersoon bij een uitings- of verspreidingsdelict. Alleen als die betrokkenheid er is of redelijkerwijs kan worden aangenomen, zijn de voorwaarden van artikel 53 van toepassing en kan de betrokken tussenpersoon door justitie worden gemaand tot de in lid 1 onder b en c bedoelde medewerking. Omgekeerd wil het feit dat de tussenpersoon zich volgens de regels van het strafrecht heeft schuldig gemaakt aan een strafbaar feit, niet zeggen dat hij daarvoor ook daadwerkelijk aansprakelijk kan worden gesteld. Artikel 53 Sr sluit, zoals in de vorige paragraaf aangegeven, vervolging uit indien aan een drietal voorwaarden is voldaan.

Een van de vragen die moeten worden beantwoord, is derhalve welke mate van verwijtbaarheid minimaal vereist is om de tussenpersoon strafrechtelijk aansprakelijk te kunnen stellen voor de inhoud van de door hem verspreide informatie. Dit is een moeilijke vraag, die tot scherpe debatten aanleiding geeft. Gelet op de massaliteit van het tegenwoordige informatieverkeer is het niet verwonderlijk dat vooral verspreiders er beducht voor zijn om verantwoordelijk te worden gehouden voor ieder bericht dat via hen wordt verspreid. Sommige Internetproviders gaan zelfs zover dat zij iedere strafrechtelijke aansprakelijkheid afwijzen, onder het motto «geen boodschap aan de boodschap». Dit standpunt leidt ertoe dat zij zich nooit schuldig zouden kunnen maken aan een strafbaar feit, ook als zij op de hoogte zouden zijn van de strafbare inhoud van materiaal dat zij doorgeven. Zo algemeen gesteld kan dit standpunt natuurlijk niet als juist worden aanvaard. De boodschapper is onder omstandigheden wel degelijk strafbaar wegens het doorgeven van bepaalde informatie. Of dit zo is, is mede afhankelijk van de reikwijdte van de betrokken strafbaarstelling. Aangezien, zoals eerder aangegeven is, de omschrijvingen van de uitings- en verspreidingsdelicten zich in de regel niet uitstrekken tot de communicatie in besloten kring, zijn degenen die die communicatie als intermediair mogelijk maken, niet aansprakelijk voor de inhoud van de communicatie. Dit geldt bijvoorbeeld voor Internetproviders voor zover zij het elektronisch postverkeer *(e-mail)* tussen individuele personen faciliteren (het posten van een e-mail in een openbare nieuwsgroep is uiteraard geen vorm van besloten communicatie). Anders ligt het echter wanneer zij een schakel zijn in de openbaarmaking en verspreiding van informatie. Dergelijke openbaarmaking en verspreiding valt doorgaans wèl onder de wettelijke omschrijving van uitings- en verspreidingsdelicten, zodat aansprakelijkheid van de tussenpersonen niet a priori kan worden uitgesloten. Zoals gezegd is daarvoor, behalve het in de delictsomschrijving omschreven handelen of nalaten, ook verwijtbaarheid vereist.

Schuld of verwijtbaarheid valt in het strafrecht uiteen in opzet – bewust, willens en wetens handelen – en schuld in de zin van *culpa* – niet-weten, maar aanmerkelijk onvoorzichtig of roekeloos handelen. Opmerking verdient dat bij de totstandkoming van de regeling van de uitgevers- en drukkersaansprakelijkheid in de vorige eeuw de meeste uitings- en verspreidingsdelicten opzettelijke delicten waren. Sindsdien zijn daaraan niet alleen nieuwe delicten toegevoegd (de discriminatiebepalingen, artikelen 240a en 240b Sr), maar hebben veel delicten ook een culpose variant gekregen (zie bijvoorbeeld de Wet van 19 juli 1934 houdende nadere voorzieningen ter bescherming van de openbare orde, Stb. 405). In potentie betekent dit een grote uitbreiding van de aansprakelijkheid van tussenpersonen. Niet langer lopen zij alleen het risico van strafrechtelijke vervolging als zij opzet (wetenschap) hebben op de (strafbare) inhoud van geschriften en andere uitingen die zij doorgeven, maar ook reeds als zij die inhoud redelijkerwijs moeten vermoeden (culpa). Deze uitbreiding van

de aansprakelijkheid van tussenpersonen betekent dat strengere eisen worden gesteld aan de zorgvuldigheid die zij bij hun werk moeten betrachten. Dit kan ertoe leiden dat zij heel voorzichtig worden en reeds bij een vermoeden dat het om een strafbare uiting gaat of dat zich onder het door hen doorgegeven materiaal een strafbare uiting bevindt – zonder dit zeker te weten – ervan afzien die uiting of dat materiaal door te geven. Ik meen dat een dergelijke houding onwenselijk is in het licht van de vrijheid van meningsuiting en niet strookt met de wens van de wetgever van 1881 om zelfcensuur van tussenpersonen zoveel mogelijk te voorkomen. Tussenpersonen dienen mijns inziens dan ook slechts aansprakelijk te worden gehouden indien bij hen opzet aanwezig is, dat wil zeggen wetenschap of kennis van de strafbaarheid van bepaald materiaal dat zij doorgeven. Pas dan kan eventueel van hen worden gevergd om maatregelen te treffen ter voorkoming van de (verdere) verspreiding van dat materiaal. Ik stel dan ook voor om in artikel 53 Sr een nieuw tweede lid op te nemen dat bepaalt dat bij de beoordeling van de strafbaarheid van de tussenpersoon alleen die uitingen in aanmerking worden genomen waarop zijn opzet was gericht. Een vergelijkbare bepaling bestaat reeds in de artikelen 47 lid 2 en 49 lid 4 Sr, waar de aansprakelijkheid van de uitlokker respectievelijk de medeplichtige nader wordt begrensd tot diens opzettelijke daden. Verder, en in overeenstemming hiermee, stel ik voor om het specifiek op de tussenpersoon betrekking hebbende strafbaar feit van artikel 418 Sr (kortweg de onzorgvuldig handelende tussenpersoon) te beperken tot opzettelijk handelen.

De beperking van de aansprakelijkheid van tussenpersonen tot opzettelijk handelen, dat wil zeggen tot de openbaarmaking of verspreiding door hen van materiaal waarvan zij de (strafbare) inhoud kennen, is naar mijn indruk in lijn met het standpunt zoals zich dat in andere landen en in internationale gremia zoals de Raad van Europa en de Europese Unie aftekent. Ik teken hierbij aan dat de gedachtenontwikkeling over deze kwestie ten gevolge van de stormachtige ontwikkelingen in de informatie- en communicatietechnologie pas kort geleden op gang is gekomen. Dat het onderhavige voorstel aansluit bij ontwikkelingen elders moge bijvoorbeeld blijken uit de recente Duitse *Informations- und Kommunikationsdienste-Gesetz,* die in artikel 1 (Teledienstegesetz), § 5, onderdeel 2, de volgende aansprakelijkheidsregeling kent: «Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten *Kenntnis* haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern» (cursivering niet origineel).

Wanneer is spake van opzet van de tussenpersoon? Bij uitgevers in de klassieke zin zal wetenschap van de inhoud van het betrokken geschrift aanwezig zijn op het moment van de publicatie, bij verspreiders als de Internetproviders, die dagelijks miljoenen berichten doorgeven, doorgaans niet. Deze laatsten kunnen echter op de hoogte komen doordat ze door een abonnee worden gewezen op een bepaald (bijvoorbeeld discriminatoir) geschrift dat zich op de computer van de provider bevindt, of via een meldpunt waar meldingen kunnen worden gedaan van de aanwezigheid op het Internet van mogelijk strafbaar materiaal. Hierbij teken ik aan dat niet steeds meteen duidelijk zal zijn dat sprake is van een strafbare uiting. Bij kinderporno zal de strafbaarheid veelal niet aan twijfel onderhevig zijn, bij (mogelijk) discriminatoire uitingen soms wel. Opzet op die strafbaarheid kan pas aanwezig worden geacht indien de tussenpersoon bewust de aanmerkelijke kans aanvaardt dat strafbare informatie door zijn tussenkomst wordt verspreid (het zogenaamd voorwaardelijk opzet). Vage aanwijzingen of vermoedens zijn daarvoor niet voldoende. Praktisch gezien ligt het in gevallen van twijfel voor de hand dat de tussenpersoon bij de officier van justitie te rade gaat en deze de vraag voorlegt of hier sprake is van strafbaar materiaal. Indien de officier aan de

tussenpersoon meedeelt van oordeel te zijn dat sprake is van strafbaar materiaal en de tussenpersoon neemt niet onmiddellijk maatregelen ter beëindiging van de verspreiding, is op dat moment ten minste sprake van voorwaardelijk opzet van de tussenpersoon op de verspreiding van strafbare uitingen. De officier van justitie zal vervolgens de tussenpersoon aanmanen (in de zin van artikel 53, eerste lid, onder b en c, Sr) aanwijzingen te geven omtrent de dader en verdere verspreiding zoveel mogelijk te voorkomen. Er is dus een duidelijk verband tussen de in artikel 53, tweede lid, voorgestelde beperking van de strafbaarheid van de tussenpersoon tot opzetgevallen en het systeem van de voorwaarden van artikel 53, eerste lid, dat de beoordeling of sprake is van strafbaar materiaal waartegen moet worden opgetreden, primair bij justitie neerlegt. Samenvattend ben ik van mening dat de eis van opzet in combinatie met de voorgestelde vervolgbaarheidsvoorwaarden een waarborg vormen dat tussenpersonen niet onnodig voorzichtig worden en overgaan tot zelfcensuur. Zelfs wanneer een tussenpersoon laakbaar in strafrechtelijke zin heeft gehandeld (dat wil zeggen er is sprake van (voorwaardelijk) opzet aan zijn kant), kan pas actie tegen hem worden ondernomen nadat hij op zijn strafbaar handelen is gewezen en in de gelegenheid is gesteld om aan de voorwaarden van artikel 53 Sr te voldoen. Dit biedt tussenpersonen de mogelijkheid om – met name in moeilijke gevallen, waarin bijvoorbeeld twijfel bestaat over de strafbaarheid van bepaalde uitingen of onduidelijk is welke maatregelen getroffen moeten worden (en door wie) om het strafbaar feit te beëindigen – daarover eerst het oordeel van de officier van justitie af te wachten. Aldus wordt tot uitdrukking gebracht dat de tussenpersoon niet op de stoel van de politie of de rechter behoeft te gaan zitten. Dit laat uiteraard onverlet dat de tussenpersoon niet gehouden is om een aanmaning van justitie af te wachten maar kan besluiten om, wanneer hij kennis krijgt van de aanwezigheid van materiaal over de strafbaarheid waarvan geen twijfel mogelijk is, daaraan eerder een eind te maken.

## 3. Vernietiging van computergegevens

*3.1 «Inbeslagneming» van computergegevens*

Door de ontwikkeling van computers en informatietechnologie is de band tussen informatie en de informatie*dragers* veel losser geworden. De nieuwe technologie maakt het mogelijk enorme hoeveelheden gegevens op te slaan zonder noemenswaardig ruimtebeslag (een enkele diskette of een harde schijf), razendsnel te verwerken en zo nodig te transporteren naar andere geautomatiseerde werken, die aan het andere eind van de wereld staan. Om deze computergegevens te kunnen lezen heeft men behalve uiteraard computers speciale programmatuur nodig en soms zelfs onstoffelijke «sleutels», wanneer de informatie is beveiligd. Een en ander heeft uiteraard gevolgen voor een informatiegevoelige sector als de opsporing. De klassieke opsporingsbevoegdheden, zoals inbeslagneming en huiszoeking, zijn in een geautomatiseerde omgeving niet steeds zonder meer toepasbaar. Deze omgeving stelt nieuwe eisen, die onder andere zijn neergelegd in Aanbeveling nr. R (95) 13 van de Raad van Europa *concerning problems of criminal procedural law connected with information technology* (aangenomen door het Comité van Ministers op 11 september 1995). Beginsel nr. 2 van het hoofdstuk over «search and seizure» luidt:

«Criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure should be equally applicable in

case of search in computer systems and in case of seizure of data therein.»

Aanbevolen wordt dus om analoog aan de traditionele zoek- en inbeslagnemingsbevoegdheden bevoegdheden te creëren die het mogelijk maken om onder gelijke voorwaarden computersystemen te doorzoeken en gegevens «in beslag» te nemen. Daarbij dient de rechtsbescherming van belanghebbenden voldoende te zijn gewaarborgd, hetgeen onder andere betekent dat geheime zoekacties naar opgeslagen informatie, zonder dat betrokkene zelfs maar op de hoogte is van het onderzoek tegen hem, niet geoorloofd zijn.
De Aanbeveling van de Raad van Europa maakt onderscheid tussen maatregelen met het oog op de waarheidsvinding en maatregelen om iets (gegevens) aan de macht van de betrokkene te onttrekken teneinde te voorkomen dat deze er (verder) misbruik van maakt of het verspreidt (zie § 54 e.v. van het *Explanatory memorandum)*, een onderscheid dat ook naar Nederlands recht relevant is (vgl. de verschillende doeleinden van inbeslagneming, artikel 94, eerste en tweede lid, Sv). De eerste Wet computercriminaliteit (Stb. 1993, 33) richtte zich met name op het eerste, de waarheidsvinding. Zo kunnen het bevel tot toegangverlening tot of overbrenging van gegevens (artikel 125i Sv) en de netwerkzoeking (artikel 125j Sv) slechts betrekking hebben op gegevens die kunnen dienen om de waarheid aan de dag te brengen. Het gaat er hierbij om om van bepaalde gegevens kennis te kunnen nemen; doel is níet om de gegevens aan de beschikkingsmacht van de betrokkene te onttrekken. Doorgaans zal dus volstaan kunnen worden met het maken van een kopie van de betrokken gegevens. Het opeisen van de originele gegevens of het wegnemen van gegevens zonder achterlating van een kopie is in strijd met de, bij iedere opsporingsbevoegdheid in acht te nemen, eisen van proportionaliteit en subsidiariteit. Zodra de bij onderzoek in geautomatiseerde werken vastgelegde gegevens van geen betekenis meer zijn voor het onderzoek, dienen ze – dat wil zeggen alleen de kopieën ten behoeve van justitie – te worden vernietigd (artikel 125n Sv).
Het Wetboek van Strafvordering voorziet dus niet in de situatie dat bij een onderzoek in een geautomatiseerd werk gegevens worden aangetroffen die voorwerp uitmaken van een strafbaar feit (bijvoorbeeld discriminerende uitlatingen (artikel 137c Sr) en bedrijfsgeheimen (artikel 273)) of met behulp waarvan een strafbaar feit is gepleegd (een computervirus, zie artikel 350a Sr). De Nederlandse justitie kan naar huidig recht weinig tegen deze gegevens uitrichten. Waar het gaat om stoffelijke voorwerpen (boeken met een strafbare inhoud, schadelijke werktuigen) beschikken de strafrechtelijke organen over de bevoegdheid tot inbeslagneming en over de sancties van verbeurdverklaring en onttrekking aan het verkeer. Waar het echter gaat om computergegevens waarmee strafbare feiten zijn gepleegd, kan de politie alleen een kopie maken met het oog op de waarheidsvinding. De toepassing van de inbeslagnemingsbevoegdheid ten aanzien van die gegevens – zodanig dat ze uit de macht van de betrokkene worden gehaald – is niet mogelijk aangezien in de visie van de wetgever gegevens geen «goed» zijn (dit is recentelijk bevestigd door de Hoge Raad, zie HR 3 december 1996, NJ 1997, 574 m.nt. 'tH). Inbeslagneming van de computer met het oog op onttrekking aan het verkeer is evenmin geoorloofd, omdat een computer op zichzelf geen verkeersgevaarlijk voorwerp is en bovendien inbeslagneming uitsluitend vanwege een in de computer aanwezig bestand als disproportioneel moet worden aangemerkt. Alleen wanneer het strafbare bestand zou zijn vastgelegd op een losse diskette, zou inbeslagneming van die diskette met het oog op onttrekking aan het verkeer wellicht verdedigbaar zijn.
Dit wetsvoorstel voorziet in de hier geschetste lacune en opent de mogelijkheid om computergegevens met betrekking tot welke of met behulp waarvan een strafbaar feit is gepleegd, bij wijze van voorlopige

maatregel ontoegankelijk te maken en bij de einduitspraak over het feit of bij afzonderlijke beschikking door de rechter te doen vernietigen. Dit voorstel is in overeenstemming met de Aanbeveling van de Raad van Europa. In de voorgestelde regeling is een aantal elementen overgenomen uit de regeling van de inbeslagneming van voorwerpen met het oog op onttrekking aan het verkeer. Gelet op de analogie ligt dit voor de hand. Wel konden de beoogde maatregelen op een aantal punten eenvoudiger worden geformuleerd. Voorts heb ik er vanaf gezien een aparte strafrechtelijke maatregel, à la de onttrekking aan het verkeer, ten aanzien van gegevens te introduceren. Gelet op het onstoffelijke karakter van gegevens en op het feit dat vermogenswaarde ervan vaak ontbreekt of moeilijk te kwantificeren is, heeft een zelfstandige sanctie ten aanzien van gegevens weinig zin.

Over de effectiviteit van de voorgestelde maatregelen van ontoegankelijkmaking en vernietiging van computergegevens merk ik nog het volgende op. De maatregelen zijn in verschillende gevallen toepasbaar. Waar het gaat om toepassing op voor een ieder beschikbare gegevens op grensoverschrijdende computernetwerken zoals Internet, is effectieve ontoegankelijkmaking bijzonder moeilijk. Dergelijke gegevens worden namelijk, juist met het oog op de toegankelijkheid voor een groot publiek, met behulp van zogenaamde *cache*-technieken op vele plaatsen in het netwerk opgeslagen. Het risico is dan aanwezig dat als gegevens op de ene plaats ontoegankelijk worden gemaakt, ze even later op een andere plaats weer opduiken. Overigens sluit ik niet uit dat de technische mogelijkheden zich zodanig zullen ontwikkelen dat het beter mogelijk wordt om ook op Internet bepaalde gegevens – en hun kopieën – op te sporen en ontoegankelijk te maken.

De voorgestelde maatregelen van ontoegankelijkmaking en vernietiging hebben echter in twee opzichten een ruimer bereik, op grond waarvan ik meen dat in het algemeen de uitvoerbaarheid en effectiviteit in voldoende mate is gegarandeerd. Ten eerste zijn ze niet alleen toepasbaar op gegevens (bijv. strafbare uitingen) die bestemd zijn voor een groot publiek en daarom, zoals hierboven aangegeven, op verschillende plaatsen in een netwerk aanwezig zijn. Ze zijn daarentegen ook toepasbaar op gegevens die slechts voor een kleine kring van personen beschikbaar zijn (bijv. bepaalde criminele computerprogramma's of ontvreemde bedrijfsinformatie die de concurrent voor zichzelf wil houden) en dus slechts op een of enkele plaatsen in een netwerk aanwezig zijn. Dergelijke computergegevens zijn eenvoudiger traceerbaar dan voor eenieder beschikbare informatie. Ten tweede zijn de maatregelen van ontoegankelijkmaking en vernietiging van computergegevens niet alleen bestemd voor toepassing in openbare, internationale netwerken, maar ook voor toepassing in op zichzelf staande (stand-alone) computers en in niet-openbare en dus kwa omvang veel kleinere netwerken zoals bedrijfsnetwerken. In die situaties is het wel degelijk mogelijk om bepaalde computergegevens op effectieve wijze ontoegankelijk te maken.

Los van de verwachte effectiviteit is er een belangrijke zelfstandige reden om de ontoegankelijkmaking en vernietiging van computergegevens in het Wetboek van Strafvordering op te nemen. Die is gelegen in het feit dat het hier om gegevens gaat die naar hun aard niet in het normale, legale verkeer aanwezig behoren te zijn, althans niet in de beschikkingsmacht van personen met kwade bedoelingen. Het gaat om de moderne varianten van «contrabande» zoals boeken met een strafbare inhoud of inbrekerswerktuig. Het is mijns inziens uit een oogpunt van geloofwaardige rechtshandhaving onbevredigend en onwenselijk dat opsporingsinstanties tegen dergelijk materiaal in computers niet kunnen optreden en het, na voldoende bewijzen te hebben verzameld, in de computer moeten laten staan.

Tot slot wijs ik er nogmaals op dat de voorgestelde maatregelen volledig in overeenstemming zijn met hetgeen in de Aanbeveling nr. R (95) 13 van de Raad van Europa is bepaald.

*3.2 Ontoegankelijkmaking en vernietiging van gegevens*

Allereerst wordt een nieuw artikel 125o Sv voorgesteld, inhoudende een bevoegdheid van de officier van justitie en de rechter-commissaris om te bepalen dat computergegevens met betrekking tot welke of met behulp waarvan het strafbaar feit is gepleegd, *ontoegankelijk worden gemaakt.* De maatregel is slechts mogelijk voor zover zij noodzakelijk is ter beëindiging van het strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Onder «ontoegankelijkmaking van gegevens» wordt verstaan het treffen van maatregelen ter voorkoming dat de beheerder van dat geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Onder ontoegankelijkmaking wordt mede verstaan het verwijderen (wissen) van de betrokken bestanden, met behoud van een kopie voor justitie (artikel 125o, tweede lid). Dit is de meest voor de hand liggende maatregel. De definitie van ontoegankelijkmaking laat daarnaast echter allerlei andere maatregelen toe, mits die kunnen strekken ter voorkoming van de verdere kennisneming enz. van die gegevens. Een voorbeeld van zulke andere maatregelen is het met behulp van zogenaamde encryptietechnieken als het ware een «slot» zetten op de betrokken bestanden, zodat de beheerder en andere gebruikers van de computer er geen toegang meer toe hebben. Daarnaast is bijvoorbeeld denkbaar dat de toegangspoort van de betrokken computer (tijdelijk) onbruikbaar wordt gemaakt. In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is. Daarbij moeten uiteraard de eisen van proportionaliteit en subsidiariteit in acht worden genomen. Dit vereist in het bijzonder in netwerkomgevingen voorzichtigheid, opdat niet onnodig schade wordt toegebracht aan gegevens of systemen. Soms zal het daarom in de rede liggen om de medewerking van de netwerkbeheerder te vragen. Deze kan daarvoor eventueel een vergoeding krijgen op grond van de Wet tarieven in strafzaken. Uiteraard zal de opsporingsambtenaar trachten alle kopieën en back-ups van de gegevens te achterhalen. De maatregel van ontoegankelijkmaking zou anders zijn effect kunnen missen. Een effectieve toepassing van de bevoegdheid betekent verder ook dat bij het wissen van het bestand op een gegevensdrager de technische voorzorgsmaatregelen moeten worden genomen om te voorkomen dat gewiste bestanden achteraf alsnog weer leesbaar worden gemaakt. Van het politie-apparaat mag worden verwacht dat het zich wat dit betreft op de hoogte houdt van de informatietechnologische ontwikkelingen en mogelijkheden en dienovereenkomstig de nodige maatregelen treft die nodig zijn om het gewenste resultaat – de beëindiging van een strafbare situatie en de voorkoming dat verder strafbaar zal worden gehandeld – te bereiken. Soms zal een externe deskundige moeten worden ingeschakeld. In bepaalde gevallen zal de politie haar huidige werkmethoden mogelijk enigszins moeten aanpassen. Zo gaat de politie er nu veelal toe over om van de volledige harde schijf van een geautomatiseerd systeem een kopie te maken teneinde die op het bureau te kunnen onderzoeken op voor de opsporing relevante gegevens. Dit kan in bepaalde situaties, waarin de ongestoorde voortgang van de bedrijfsvoering in het geding is, een legitieme en evenredige methode van onderzoek zijn (zolang deze gegevens niet ook voor andere doeleinden worden gebruikt). Zij doet echter afbreuk aan de effectiviteit van de voorgestelde maatregel van ontoegankelijkmaking van bepaalde gegevens, aangezien zij de verdachte de tijd geeft om bepaalde bestanden van zijn harde schijf te verwijderen. In zo'n situatie zal de politie dus ter plaatse moeten trachten strafbare bestanden te achterhalen en – met

toestemming van de officier van justitie of de rechter-commissaris – daartegen de noodzakelijke maatregelen moeten treffen. Ik realiseer me dat dit met name in «netwerkomgevingen» niet altijd een eenvoudige opgave zal zijn.
De bevoegdheid tot ontoegankelijkmaking is voorbehouden aan de officier van justitie dan wel, tijdens een gerechtelijk vooronderzoek, de rechter-commissaris. Dit sluit aan bij de bevoegdheidstoedeling in de huidige zevende afdeling van titel IV van boek 1 en waarborgt dat wanneer bij een onderzoek in een computer door een opsporingsambtenaar (in zijn ogen) dubieuze gegevens worden aangetroffen, deze gegevens niet rauwelings ontoegankelijk kunnen worden gemaakt. Daarvoor is een afstandelijk oordeel, van een officier van justitie of een rechter-commissaris, vereist.
Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen waarmee de gegevens ontoegankelijk zijn gemaakt, dienen de officier van justitie dan wel de rechter-commissaris een daartoe strekkende opdracht te geven. Wordt de ontoegankelijkmaking van de gegevens ongedaan gemaakt, dan herleeft de beschikkingsmacht van degene in wiens computer de gegevens waren aangetroffen. Dit kan op één lijn worden gesteld met de teruggave van een inbeslaggenomen voorwerp aan de beslagene. Ingeval de betrokken bestanden door de politie uit de computer van de betrokkene zijn verwijderd, dient een kopie te worden teruggegeven. Teruggave (dat wil zeggen opheffing van de ontoegankelijkmaking) zal overigens ook moeten geschieden indien de rechter later in de hoofdzaak mocht besluiten om de betrokken gegevens toch niet te laten vernietigen, bijvoorbeeld omdat hij ze niet strafbaar acht, of indien de rechter daartoe beslist op het beklag van een belanghebbende op grond van artikel 552a Sv (zie verderop).
De ontoegankelijkmaking is een voorlopige maatregel. In het nieuwe artikel 354 Sv wordt voorgeschreven dat de rechter bij een materiële einduitspraak over het feit (dat wil zeggen een veroordeling, een vrijspraak of een ontslag van rechtsvervolging) een definitieve beslissing neemt over de ontoegankelijk gemaakte gegevens, voor zover deze maatregel nog niet door de officier van justitie of de rechter-commissaris is opgeheven. Als hij vaststelt dat de voorwaarden daarvoor aanwezig zijn, kan hij gelasten dat de betrokken computergegevens worden vernietigd. De voorwaarden zijn dezelfde als voor de ontoegankelijkmaking, dat wil zeggen dat het moet gaan om gegevens met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan en dat de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten. In alle andere gevallen gelast de rechter de opheffing van de ontoegankelijkmaking. Niet voorzien is in de mogelijkheid voor de officier van justitie om in het kader van een transactie als voorwaarde te stellen dat de verdachte afstand doet van computergegevens die vatbaar zijn voor vernietiging op last van de rechter (vgl. ten aanzien van voorwerpen artikel 74, tweede lid, onder b, Sr). De voorgestelde bevoegdheid dient aan de onafhankelijke rechter te worden voorbehouden, reeds omdat artikel 7 van de Grondwet eist dat elke inhoudelijke beperking van de vrijheid van meningsuiting die zich in het concrete geval effectueert, moet kunnen worden voorgelegd aan de onafhankelijke rechter; dit ligt besloten in de woorden «behoudens ieders verantwoordelijkheid volgens de wet». Wat de rechtsbescherming tegen maatregelen tot ontoegankelijkmaking betreft, wordt bepaald dat belanghebbenden zich met een klacht over de ontoegankelijkmaking kunnen wenden tot de raadkamer. Hiertoe wordt de beklagmogelijkheid van artikel 552a Sv uitgebreid. Dit is in overeenstemming met Aanbeveling R (95) 13 van de Raad van Europa, die voorschrijft dat de rechtsmiddelen die bestaan ten aanzien van onderzoek ter inbeslagneming van voorwerpen, van overeenkomstige toepassing zijn ten aanzien van het onderzoek in computers.
De rechterlijke last tot vernietiging zal doorgaans meebrengen dat alle bij

justitie berustende kopieën worden vernietigd. Indien de gegevens ook nog aanwezig zijn in de computer van de betrokkene – zij het door justitie ontoegankelijk gemaakt door middel van encryptietechnieken –, zullen ook deze moeten worden vernietigd.

*3.3 De voorwaarden voor ontoegankelijkmaking en vernietiging*

De ontoegankelijkmaking en uiteindelijke vernietiging van computergegevens dient een tweeledig doel: beëindiging van het strafbaar feit en voorkoming dat met de betrokken gegevens nieuwe strafbare feiten worden gepleegd. Het tweede (preventie) ligt in het verlengde van het eerste (reparatie). Waar sprake is van een voortdurende strafbare toestand vallen beide in feite samen: de ontoegankelijkmaking van de betrokken gegevens maakt een eind aan het strafbaar feit en voorkomt tevens voortzetting daarvan. Waar daarentegen sprake is van een strafbaar feit van voorbijgaande aard (openbaarmaking van strafbare uitlatingen, bekendmaking van bedrijfsgeheimen), valt niets meer te repareren en treedt het preventieve oogmerk van de ontoegankelijkmaking van gegevens op de voorgrond, zij het dat wel is vereist dat met die gegevens een strafbaar feit is gepleegd. Dit betekent dat indien bijvoorbeeld in een *e-mail-box* racistische uitingen worden aangetroffen, dit op zichzelf nog geen grond is om de betrokken gegevens ontoegankelijk te maken en eventueel door de strafrechter te laten vernietigen. Er is immers nog geen reden om aan te nemen dat er iets strafbaars met die gegevens is gebeurd: elektronische post is een vorm van privé-verkeer die niet bestreken wordt door de artikelen 137c Sr e.v. Pas als er wel een redelijk vermoeden is dat met die gegevens op strafbare wijze is gehandeld (bijvoorbeeld door ze uit te printen en vervolgens te verspreiden), is er (voldoende) grond om ze ontoegankelijk te maken teneinde ze eventueel door de rechter te doen vernietigen.
Er zijn twee categorieën gegevens die zich lenen voor ontoegankelijkmaking c.q. vernietiging in de hier bedoelde zin: gegevens met betrekking tot welke en gegevens met behulp waarvan het strafbaar feit is begaan. Bij de eerste categorie gaat het om gegevens die «voorwerp» zijn van een strafbaar feit, om gegevens die de kern uitmaken van het feit. Hierbij moet allereerst worden gedacht aan gegevens van strafbare aard, dat wil zeggen gegevens die wegens hun aard niet mogen worden openbaar gemaakt of verspreid; dit zijn de strafbare uitingen. Daarnaast behoren tot deze categorie de gegevens die weliswaar op zichzelf volstrekt geoorloofd zijn, maar ten aanzien waarvan bepaalde handelingen strafbaar zijn gesteld zoals de opzettelijke inbreuk op eens anders auteursrecht. Hieronder valt ook de «gestolen» informatie: ontvreemde diskettes met vertrouwelijke informatie of gegevens uit een geautomatiseerd werk die door werknemers met schending van hun geheimhoudingsplicht aan anderen worden doorgespeeld. Voor zover het «bezit» of de bekendmaking of verspreiding van dergelijke gegevens strafbaar is (vgl. «heling» van bedrijfsgeheimen (artikel 273, eerste lid, onder 2, Sr) of het wederrechtelijk bezit of doorgeven van staatsgeheimen (artikelen 98 en 98c Sr)), kunnen ze bij een onderzoek in een geautomatiseerd werk ontoegankelijk worden gemaakt ter voorkoming van verder misbruik.
De tweede categorie – gegevens met behulp waarvan een strafbaar feit is begaan – betreft criminele werktuigen bestaande uit gegevensbestanden of computerprogramma's. Voorbeelden hiervan zijn boekhoudprogramma's die standaard een bepaald percentage van een transactie buiten de administratie houden, en virusprogramma's. Het is gewenst dat wanneer politie en justitie bij een onderzoek in een geautomatiseerd werk op dergelijke gegevens stuiten, zij daartegen kunnen optreden, net als het geval is bij inbrekerswerktuigen.
Tot slot wijs ik erop dat de bevoegdheid tot ontoegankelijkmaking geen verplichting inhoudt, maar een discretionaire bevoegdheid waarvan de

uitoefening aan de eisen van proportionaliteit en subsidiariteit is gebonden. Ingeval bijvoorbeeld bestanden met (ontvreemde) staatsgeheimen worden aangetroffen bij een krantenuitgeverij, zal ontoegankelijkmaking onder omstandigheden niet meer geoorloofd zijn, indien de gegevens reeds ruim bekend zijn gemaakt en de maatregel in een democratische samenleving niet (meer) noodzakelijk kan worden geacht voor het bereiken van het beoogde doel. Vgl. het arrest van het Europese Hof voor de rechten van de mens in de zaak van het Weekblad Bluf! (EHRM 9 februari 1995, Series A, no. 306-A, NJCM-Bulletin 20-4 (1995), p. 480 e.v.).

## 4. Medewerking aan de ontsleuteling van gegevens

Cryptografie is de techniek van het geheimschrift. In de informatietechnologie worden cryptografische technieken gebruikt om gegevens en boodschappen te versleutelen (vercijferen) ter verzekering van de vertrouwelijkheid van die gegevens. Het spreekt voor zich dat het gebruik van cryptografie door criminelen politie en justitie kan hinderen bij de waarheidsvinding. Met het oog daarop is dan ook bij de Wet computercriminaliteit in artikel 125k, tweede lid, van het Wetboek van Strafvordering de bevoegdheid opgenomen om personen die kennis dragen van de versleuteling van gegevens, te verplichten medewerking te verlenen aan de waarheidsvinding door deze kennis ter beschikking te stellen van justitie. Deze bevoegdheid heeft betrekking op onderzoek ter gelegenheid van een huiszoeking naar gegevens die zijn *opgeslagen* in een geautomatiseerd werk. Artikel 125k ziet niet op het onderzoek naar *stromende* gegevens, de telecommunicatie. Dit onderzoek van telecommunicatie is geregeld in het huidige artikel 125g betreffende de tapbevoegdheid; ingevolge de Wet bijzondere opsporingsbevoegdheden[3] zal het in de 126m en 126t Sv worden geregeld). Anders dan bij de huiszoeking bestaat ten aanzien van het aftappen van telecommunicatie nog geen mogelijkheid voor justitie om de medewerking van derden af te dwingen bij het ontsleutelen van gegevensverkeer. Dit wetsvoorstel voorziet hierin door een aanvulling van de artikelen 126m en 126t Sv analoog aan artikel 125k: tot degeen van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van telecommunicatie, kan het bevel worden gericht mee te werken aan het ontsleutelen van de betrokken gegevens. Deze bevoegdheid strekt ertoe kennis te kunnen nemen van gegevens die anders voor de strafvorderlijke autoriteiten wartaal zouden blijven. Het bevel wordt, conform het stelsel voorzien bij de Wet bijzondere opsporingsbevoegdheden, gegeven door de officier van justitie, die in dat stelsel de bevoegde autoriteit is ten aanzien van het tappen. Voor het geven van zo'n bevel heeft hij de (schriftelijke) machtiging van de rechter-commissaris nodig.
Het bevel kan, afhankelijk van de omstandigheden, worden gericht tot bijvoorbeeld de afzender van een bericht, een netwerkbeheerder of een aanbieder van een telecommunicatienetwerk ofdienst: tot een ieder van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van bepaalde afgetapte telecommunicatie. Dit zou ook een zogenaamde Trusted Third Party (TTP) kunnen zijn, een bedrijf dat behulpzaam is bij het verzekeren van de betrouwbaarheid van elektronisch gegevensverkeer (bijvoorbeeld door langs elektronische weg de integriteit van een bepaald bestand te verzekeren of de identiteit van een andere partij vast te stellen). Voor zover zo'n TTP kennis draagt van de door een klant toegepaste encryptietechnieken (mogelijk voor deze de sleutel bewaart), kan het verplicht worden die kennis ter beschikking van justitie te stellen.
De medewerkingsverplichting strekt zich alleen uit tot die kennis waarvan redelijkerwijs kan worden vermoed dat zij bij de betrokkene aanwezig is. Het gaat, met andere woorden, om het ter beschikking stellen van

[3] De wet van 27 mei 1999 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden) (Stb. 245). Deze wet is nog niet in werking getreden.

*beschikbare* kennis of het aanwenden van beschikbare technieken. In het algemeen zal dit betekenen dat iemand slechts verplicht kan worden die versleuteling ongedaan te maken die hij zelf heeft aangebracht of die sleutel te verstrekken waarover hij zelf beschikt. Het betekent ook dat wie niet over de benodigde kennis of technieken beschikt om te kunnen ontsleutelen, niet op grond van de voorgestelde medewerkingsverplichting gehouden is, daarnaar onderzoek te doen en instrumenten te ontwikkelen om toch te kunnen ontsleutelen. Evenmin kan van zoiemand worden geëist dat hij alsnog de benodigde technische voorzieningen installeert. Tot slot impliceert de voorgestelde medewerkingsverplichting geen sleutelbewaarplicht: wie feitelijk niet meer in staat is om mee te werken aan de ontsleuteling omdat hij niet meer over de sleutel beschikt, is ontslagen van zijn meewerkplicht.
De sleutel tot het ontcijferen van informatie kan voor de houder ervan van grote waarde zijn. Hij kan er belang bij hebben de kennis daaromtrent niet verder te verspreiden dan strikt nodig is. De voorgestelde bepaling voorziet daarom in de mogelijkheid dat de houder, naar zijn keuze, niet de sleutel ter beschikking stelt, doch deze zelf hanteert om het versleutelde signaal te ontcijferen. Overigens worden de kosten die in het concrete geval moeten worden gemaakt voor de medewerking, vergoed ingevolge de Wet tarieven in strafzaken.
De voorgestelde medewerkingsverplichting ten aanzien van het ontsleutelen van telecommunicatie laat onverlet de specifieke verplichtingen die ingevolge de nieuwe Telecommunicatiewet op aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten rusten. Deze verplichtingen overlappen elkaar gedeeltelijk. Artikel 13.1, eerste lid, van de Telecommunicatiewet bepaalt namelijk dat telecomaanbieders hun netwerken en diensten uitsluitend aan gebruikers beschikbaar mogen stellen indien die netwerken en diensten aftapbaar zijn. Deze algemene eis omvat onder andere de plicht voor de aanbieder om zijn netwerk of dienst zodanig in te richten dat de telecommunicatie die door middel van aftappen is verkregen, alvorens deze aan de bevoegde instanties wordt doorgegeven, door hem wordt ontdaan van de eventueel door hemzelf toegepaste cryptografie en andere bewerkingen. Deze eis zal worden neergelegd in een algemene maatregel van bestuur op grond van artikel 13.1, tweede lid, Telecommunicatiewet. Indien derhalve een telecommunicatieaanbieder op basis van het Wetboek van Strafvordering wordt bevolen mee te werken aan het aftappen of opnemen van door hem verzorgde telecommunicatie, behoeft hem niet afzonderlijk bevel te worden gegeven de door hemzelf aangebrachte versleutelingen ongedaan te maken. Dit laat onverlet dat op het betrokken gegevensverkeer meer versleutelingen kunnen zijn toegepast door verschillende andere dienst- of netwerkaanbieders. Om een dergelijke keten van versleutelingen ongedaan te maken, zal eventueel aan ieder van die andere personen op basis van de hier voorgestelde bepalingen een bevel tot medewerking kunnen worden gegeven.
Ik heb overwogen het mogelijk te maken dat een bevel tot medewerking aan de ontsleuteling van gegevens ook tot de verdachte zou kunnen worden gericht. In het ontwerp van dit wetsvoorstel dat ter consulatie aan een aantal organen is rondgezonden, was een dergelijke mogelijkheid – onder beperkende voorwaarden – opgenomen. Daarop is van verschillende kanten kritiek gekomen. De Nederlandse Vereniging voor Rechtspraak is er niet zeker van of het voorstel in overeenstemming is met het uit artikel 6 EVRM voortvloeiende recht van de verdachte «to remain silent and not tot incriminate himself» (het zogenaamd nemo-teneturbeginsel) en meent dat het nadere bestudering behoeft. De Nederlandse Orde van Advocaten gaat nog een stap verder en meent dat door het voorstel «een kritische grens (wordt) gepasseerd en daardoor de deur (wordt) opengezet voor vele andere vormen van verplicht meewerken door de verdachte.» In de wetenschappelijke wereld zijn de meningen verdeeld. Prof. Buruma

acht het in zijn preadvies voor de NJV-vergadering van 1998 («Internet en strafrecht») niet in strijd met het nemo-teneturbeginsel om de verdachte bij wet te verplichten de sleutel tot een encryptieprogramma te verstrekken. Op die vergadering waren Kuitenbrouwer en De Roos echter zeer kritisch.
Bij nader inzien ben ik van oordeel dat het verplichten van de verdachte tot medewerking aan ontsleuteling een stap te ver gaat. Bij de meeste encryptieprogramma's zal dit namelijk neerkomen op het verplicht vertellen van een slechts in het geheugen van de verdachte «opgeslagen» code of wachtwoord. Hiermee is de verklaringsvrijheid en het zwijgrecht van de verdachte in het geding. Ook de verhouding tot de beslissing van het Europese Hof voor de rechten van de mens in de zaak Saunders (EHRM 17 december 1996) is bij nader inzien niet geheel duidelijk. Enerzijds is de door het Hof aangegeven ratio van het nemo-teneturbeginsel – namelijk dat verklaringen die onder dwang zijn verkregen, mogelijk onjuistheden bevatten en minder betrouwbare informatie opleveren – bij het vragen van een cryptografische sleutel niet in het geding: de juistheid van de opgegeven sleutel kan onmiddellijk worden geverifieerd door toepassing op de versleutelde gegevens. Anderzijds sluit het Hof van het bereik van het beginsel alléén uit materiaal dat «onafhankelijk van de wil van de verdachte» bestaat en daarvan is bij een door de verdachte zelf gekozen en slechts in zijn geheugen opgeslagen wachtwoord uiteraard geen sprake. De voorgestelde artikelen 126m, zesde lid, en 126t, zesde lid, Sv bepalen dan ook dat het bevel tot medewerking niet wordt gegeven aan de verdachte.

## 5. Het onderscheid tussen opgeslagen en stromende gegevens

*5.1 Opgeslagen tegenover stromende gegevens; kritiek*

Op verschillende plaatsen in het straf(proces)recht zoals dat luidt sinds de eerste Wet computercriminaliteit speelt het onderscheid tussen opgeslagen gegevens enerzijds en stromende gegevens (of gegevens in transport) anderzijds een rol. Soms volgt dit onderscheid uit de wettekst zelf, soms uit de achterliggende ratio. In de consultatieronde van het ontwerp van het onderhavige wetsvoorstel is door verschillende instanties (Registratiekamer, Beleidsadviesgroep digitaal rechercheren van de politie, Stuurgroep Informatietechnologie en Criminaliteit) kritiek geuit op (handhaving van) dit onderscheid. Het zou niet passen bij de huidige stand van de techniek, waarbij transport en opslag moeilijk uit elkaar te houden zouden zijn (een e-mail die van A naar B wordt gezonden, wordt bijvoorbeeld soms om technische redenen tijdelijk op een tussenliggende computer opgeslagen). Er zou sprake zijn van een toenemende convergentie van opslag en transport van gegevens, die het maken van een juridisch onderscheid niet meer rechtvaardigt.
Een voorbeeld van dit onderscheid, dat mogelijk als enigszins willekeurig kan worden aangemerkt, betreft artikel 138a, tweede lid, Sr, dat met een verhoogd strafmaximum strafbaar stelt de computervredebreuk indien de dader vervolgens gegevens die *zijn opgeslagen* in het geautomatiseerd werk (...), overneemt en voor zichzelf of een ander vastlegt. Wat nu, als gedurende de tijd dat de dader zich in de computer bevindt, nieuwe gegevens binnenkomen (bijvoorbeeld via e-mail) en hij ook deze voor zichzelf overneemt? Zijn dit *opgeslagen* gegevens in de zin van het huidige artikel 138a Sr? Zo niet – de wetgever van 1993 heeft waarschijnlijk niet aan deze situatie gedacht –, wat is dan de rechtvaardiging om computervredebreuk gevolgd door het overnemen van (toe)stromende gegevens niet even zwaar te straffen als computervredebreuk gevolgd door het overnemen van reeds opgeslagen gegevens? Een rechtvaardiging daarvoor ligt niet meteen voor de hand.
Een ander voorbeeld betreft onduidelijkheid over het toepassingsbereik

van artikel 125i Sv (de bevoegdheid van de rechter-commissaris om te bevelen dat hij van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens die «zijn opgeslagen, worden verwerkt of overgedragen met gebruikmaking van een geautomatiseerd werk», deze gegevens aan de RC verstrekt) en de afbakening van die bevoegdheid ten opzichte van de bevoegdheid tot het opnemen van telecommunicatie. Mag artikel 125i Sv worden gebruikt om een Internet Service Provider te verplichten gedurende enige tijd binnenkomende en uitgaande e-mails van een bepaalde abonnee van die provider – gegevens dus die ten tijde van het bevel nog niet bestaan – ten behoeve van justitie vast te leggen? Hoewel de wettekst een dergelijk gebruik van artikel 125i niet uitsluit, zal daaraan bij de totstandkoming van de eerste Wet computercriminaliteit niet zijn gedacht. Artikel 125i is oorspronkelijk immers bedoeld als moderne pendant van de bevoegdheid tot het vorderen van de uitlevering van voor inbeslagneming vatbare voorwerpen (zie artikel 105 Sv): waar voorheen de uitlevering van bepaalde fysieke geschriften, zoals boeken en ordners, werd gevorderd, moet bij de huidige automatisering van bedrijfsprocessen vaak de verstrekking van bepaalde in computers opgeslagen gegevens worden gevorderd.

Vooropgesteld dient te worden dat de in de strafwet gehanteerde termen en begrippen zo veel mogelijk moeten aansluiten bij de maatschappelijke realiteit (daaronder begrepen de technische realiteit). Dit laat onverlet dat begrippen in het recht niet steeds dezelfde betekenis behoeven te hebben als in andere disciplines, aangezien de juridische begrippen moeten worden uitgelegd in het licht van de functie die ze hebben bij de regulering van het maatschappelijk verkeer. Het gaat, met andere woorden, bij in de strafwet gehanteerde begrippen als «opgeslagen» en «overgedragen» (gegevens) om de maatschappelijke functionaliteit van de betrokken bepalingen en veel minder om de technische functionaliteit. Ook de Nota Wetgeving voor de elektronische snelweg stelt dat een wettelijk onderscheid tussen opgeslagen gegevens en gegevens in transport nog steeds gerechtvaardigd kan zijn, waarbij wordt aangetekend dat met name het juridisch gebruik van het begrip «transport» een invulling moet krijgen die abstraheert van de precieze technische gang van zaken.

Verder dient voorop te staan dat het in het strafrecht zo centrale legaliteitsbeginsel eist dat zowel strafbepalingen als strafvorderlijke bevoegdheden zo nauwkeurig mogelijk worden omschreven. Reeds op grond van dit uitgangspunt ben ik geen voorstander van het loslaten van de thans onderscheiden termen als «opgeslagen», «overdragen», «vastleggen», «aftappen of opnemen». Hiervoor in de plaats zouden immers ruimere, abstractere termen moeten komen, die voor de burger en voor de opsporingsambtenaar minder duidelijkheid zouden brengen. Hierbij komt nog dat het loslaten van het onderscheid opslag-transport zeker voor het Wetboek van Strafvordering zou betekenen dat een geheel nieuwe regeling van bevoegdheden zou moeten worden ontworpen (in concreto zouden de afdelingen zes en zeven van titel IV van het Eerste Boek ingrijpend moeten worden herzien en wellicht zelfs in elkaar geschoven). Dit is mijns inziens uit een oogpunt van rechtszekerheid evenmin aantrekkelijk.

Hiermee is nog niet gezegd dat sprake is van een fundamenteel onderscheid (tussen opgeslagen gegevens en gegevens in transport), dat als het ware het hele strafrecht doortrekt. Per situatie moet de wetgever bezien wat hij strafbaar wil stellen dan wel waartoe hij een opsporingsambtenaar of een andere autoriteit bevoegd wil maken (heeft het betrekking op opgeslagen gegevens of op gegevens in transport of op beide?) en daarop zijn terminologie afstemmen. Dit is in dit wetsvoorstel geschied en heeft geleid tot een aantal aanpassingen van bepalingen uit beide wetboeken, die hieronder worden toegelicht.

Het onderhavige wetsvoorstel gaat uit van een terminologie die, naar ik meen, enerzijds goed aansluit bij de maatschappelijke werkelijkheid en het normale spraakgebruik en dus de praktijk voldoende houvast biedt en anderzijds voldoende onderscheidend vermogen heeft om strafbepalingen en strafvorderlijke bevoegdheden precies te omschrijven. De gehanteerde termen komen grotendeels ook reeds in de bestaande strafwet voor zij het dat ze daarin niet altijd even consequent zijn toegepast.
Waar het gaat om reeds bestaande, in een computer opgeslagen gegevens, wordt in dit wetsvoorstel de term «opgeslagen» gehanteerd, waar het gaat om stromende gegevens de termen «(worden) verwerkt of overgedragen». Maakt het niet uit of het gaat om opgeslagen gegevens dan wel om stromende gegevens, dan wordt de trits «(zijn) opgeslagen, (worden) verwerkt of overgedragen» gebruikt. Zie als voorbeeld van dit laatste het voorgestelde artikel 138a, tweede lid, Sr, volgens welk het verhoogde strafmaximum voortaan van toepassing is indien de dader gegevens die *zijn opgeslagen, worden verwerkt of overgedragen* door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt. Zoals hierboven reeds is aangegeven maakt het voor de strafwaardigheid niet uit of de hacker reeds bestaande, opgeslagen gegevens overneemt dan wel de tijdens de inbraak binnenkomende gegevens opneemt. De termen «verwerken» en «overdragen» overlappen elkaar ten dele. Waar «overdragen» echter ziet op het transport van A naar B, omvat «verwerken» daarnaast ook bewerkingen van gegevens binnen één computer. «Verwerken» heeft hier overigens niet geheel dezelfde betekenis als in het voorstel voor een Wet bescherming persoonsgegevens (kamerstukken II 1997/98, 25 892, nrs. 1–2), waar de term niet alleen geautomatiseerde handelingen ten aanzien van (persoons)gegevens omvat maar ook iedere menselijke handeling, hetgeen uiteraard uit de strekking van die wet voortvloeit. Gehandhaafd blijven verder de termen «aftappen of opnemen». Deze hebben in de strafwet reeds een min of meer vastomlijnde betekenis en worden gebruikt voor het onderscheppen en vastleggen van stromende gegevens (vgl. artikelen 125g Sv en 139a e.v. Sr). In het wetsvoorstel wordt deze terminologie voortgezet. Ter onderscheiding van «aftappen of opnemen» wordt waar het gaat om het kopiëren van bestaande, opgeslagen gegevens, de term «overnemen» gebruikt. De termen «kennisnemen» en «vastleggen», tot slot, worden in neutrale zin gebruikt en kunnen zowel op opgeslagen als op stromende gegevens betrekking hebben.
In de artikelsgewijze toelichting zullen de terminologische aanpassingen per bepaling worden aangegeven. In algemene zin zij daarover nog het volgende opgemerkt.
In het materiële strafrecht blijkt het onderscheid tussen opgeslagen en stromende gegevens niet steeds even relevant en maakt het niet wezenlijk uit of een bepaalde (strafwaardige) handeling plaatsvindt ten aanzien van het een of het ander. Een belangrijke uitzondering wordt gevormd door de artikelen 139a e.v. Sr, die straf stellen op overtreding van de zogenaamde aftap- en opneemverboden: deze strafbepalingen zijn en blijven in dit voorstel gereserveerd voor het onderscheppen van gegevens in transport. Het is onnodig om deze bepalingen uit te breiden tot het (met een technisch hulpmiddel) overnemen of kopiëren van in computers opgeslagen gegevens omdat dit reeds omvat wordt door de strafbaarstelling van computervredebreuk (gevolgd door het overnemen van in de computer aanwezige gegevens, zie artikel 138a, tweede lid, Sr). Wel bleek het nodig het reeds bestaande bijzondere aftapverbod voor een persoon, werkzaam bij een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, uit te breiden tot het door een dergelijk persoon

zonder toestemming van de rechthebbende kennisnemen van niet voor hem bestemde gegevens die zijn opgeslagen in de computer van die telecommunicatieaanbieder (zie het voorgestelde artikel 273d Sr en nader de volgende paragraaf).
Ook (of: juist) in het Wetboek van Strafvordering komt het aan op een precieze omschrijving van de handelingen en situaties waarop men het oog heeft. Ook daarbij is het onderscheid tussen opgeslagen gegevens en stromende gegevens wellicht minder essentieel dan de wetgever van enkele jaren geleden dacht. Wel kan het onderscheid helpen de grenzen en beperkingen van strafvorderlijke bevoegdheden te verhelderen. Liever dan over opgeslagen-stromende gegevens spreek ik in dit verband echter over enerzijds het onderzoek naar reeds bestaande gegevens en anderzijds het onderzoek gedurende een zekere tijd naar gegevens die op het moment van aanvang van het onderzoek nog niet bestaan (dat wil zeggen toekomstige gegevens). Een kenmerkend voorbeeld van dit laatste type onderzoek – ook wel *real time*- onderzoek genoemd – is het aftappen van telecommunicatie. Het bedoelde onderscheid kan gevolgen hebben voor de rechtswaarborgen die moeten worden verbonden aan de toepassing van de betrokken bevoegdheden ten aanzien van de burger. Zo geldt voor bevoegdheden die betrekking hebben op toekomstige gegevens, dat ze slechts effectief zijn zolang degenen op wie ze worden toegepast, daarvan niet op de hoogte zijn (wie weet dat zijn telefoonlijn wordt afgetapt, zal daarvan geen gebruik meer maken). Bij dit soort bevoegdheden is geheimhouding dus – onder voorwaarden en gedurende een beperkte periode – gerechtvaardigd. Dit is in zijn algemeenheid anders – en geheimhouding is in beginsel dus niet gerechtvaardigd – bij bevoegdheden die betrekking hebben op bestaande gegevens: bij die gegevens bestaat immers niet het risico dat ze verloren gaan zodra de bevoegdheidsuitoefening bekend wordt. Het klassieke voorbeeld van dit soort onderzoek is de huiszoeking. Op de algemene regel bij dit soort onderzoek – geen geheimhouding – zijn overigens uitzonderingen mogelijk, in het bijzonder wanneer het nodig is om de resultaten van het onderzoek (tijdelijk) geheim te houden voor derden. In zoverre is het derhalve mogelijk dat bevoegdheden betreffende bestaande gegevens en bevoegdheden betreffende toekomstige gegevens soms op eenzelfde manier zullen worden geregeld. Ook het in de vorige paragraaf besproken voorstel om, analoog aan de reeds bestaande ontsleutelingsverplichting bij huiszoeking (artikel 125k Sv), eenzelfde verplichting op te nemen ten aanzien van het aftappen van telecommunicatie is daarvan een voorbeeld. Dergelijke aparte maar wel vergelijkbare regelingen verdienen mijns inziens echter nog altijd de voorkeur boven het formuleren van zeer algemene bevoegdheden, die zowel op bestaande als op toekomstige gegevens zien.
Ook eerdergenoemde Aanbeveling Nr. R (95) 13 van de Raad van Europa betreffende problemen van strafprocesrecht in verband met informatietechnologie maakt een duidelijk onderscheid tussen het strafvorderlijke onderzoek van gegevens opgeslagen in een computer enerzijds en het – real time – onderzoek van gegevens tijdens hun transport anderzijds. Uitgangspunt nr. 1 van de Aanbeveling schrijft voor dit onderscheid duidelijk in de wetgeving tot uitdrukking te brengen. Dit brengt mij ertoe voor te stellen om de bevoegdheid tot het opnemen van telecommunicatie enerzijds (artikel 125g Sv, zie de artikelen 126m en 126t volgens de Wet bijzondere opsporingsbevoegdheden) en de bevoegdheid van de rechter-commissaris om van betrokkenen te vorderen dat zij bepaalde computergegevens voor hem overnemen, hem daartoe toegang verlenen enz. (artikel 125i Sv) anderzijds beter ten opzichte van elkaar af te bakenen. Zoals in de vorige paragraaf aangegeven is deze verhouding onder de huidige tekst van artikel 125i niet duidelijk. Voor de toekomst wordt voorgesteld om de bevoegdheid van artikel 125i Sv te reserveren voor het onderzoek naar gegevens «die ten tijde van het bevel (van de RC)

zijn opgeslagen» in het betrokken geautomatiseerd werk, voor onderzoek naar bestaande gegevens dus. Artikel 125g is in dit stelsel bedoeld voor elk onderzoek waarbij met een technisch hulpmiddel gedurende een bepaalde periode gegevens die door middel van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst van A naar B worden getransporteerd, worden onderschept op het moment dat ze worden verwerkt of overgedragen. Dat daarbij op het moment van onderschepping in technische zin sprake kan zijn van (een kort moment van) opslag van de betrokken gegevens op een «station» tussen A en B, is niet relevant aangezien functioneel gezien sprake is van het onderscheppen (aftappen of opnemen) van toekomstig gegevensverkeer. Evenzo zal het door een ISP gedurende een bepaalde periode opnemen van gegevens op of vlak na het moment dat ze op zijn computer aankomen en daarop worden opgeslagen, als het opnemen van telecommunicatie in de zin van artikel 125g Sv moeten worden gekwalificeerd. Het gewijzigde artikel 125i Sv is daarop niet van toepassing. Overigens is onder de nieuwe Telecommunicatiewet de medewerking van ISP's aan het aftappen van e-mail verzekerd.

## 6. Onderzoek van e-mail

*6.1 (Grond)wettelijke bescherming van e-mail*

Het gebruik van *e-mail* – elektronische post, dat wil zeggen berichten die via computernetwerken worden verzonden – heeft een hoge vlucht genomen. Het maatschappelijke en economische belang van een ongehinderde communicatie door middel van e-mail lijkt inmiddels niet geringer te zijn dan dat van brief, telefoon of fax. Daardoor is ook de vraag naar de juridische bescherming van e-mail actueel geworden. Door de voortschrijdende technologische ontwikkelingen is het huidige artikel 13 Grondwet, waarin het brief-, telefoon- en telegraafgeheim is opgenomen, gedateerd geworden. Hoewel een aantal nieuwe communicatiemiddelen met extensieve interpretatie onder de werking van artikel 13 Grondwet kan worden gebracht, geeft dat toch onvoldoende zekerheid. Halverwege 1997 is dan ook een wetsvoorstel tot wijziging van artikel 13 aan de Tweede kamer aangeboden (kamerstukken 1996/97, 25 443, nrs. 1–2), dat inhield dat het bestaande brief-, telefoon- en telegraafgeheim zou worden vervangen door een algemeen recht op vertrouwelijke communicatie. Het wetsvoorstel werd in de Tweede Kamer ingrijpend geamendeerd. In de nieuwe tekst, die op 21 januari 1998 door de Tweede Kamer werd aanvaard, werd het bestaande brief-, telefoon- en telegraafgeheim op de oude voet beschermd, maar werd daarnaast bescherming verleend aan daarmee vergelijkbare communicatietechnieken. In de Eerste Kamer bleken vervolgens ernstige bezwaren te bestaan tegen dit wetsvoorstel zoals het inmiddels luidde. Naar aanleiding daarvan heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties een commissie belast met de opdracht een advies uit te brengen inzake de gevolgen van nieuwe informatie- en communicatietechnologie voor de grondrechten (de commissie «Grondrechten in het digitale tijdperk»). Omdat het in de rede ligt dat naar aanleiding van het advies van deze commissie een nieuw, meer omvattend voorstel zal worden ingediend, heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties vervolgens besloten wetsvoorstel 25 443 in te trekken. Dit laat onverlet dat de gedachtewisseling rond dit wetsvoorstel op het punt van de bescherming van e-mail nog steeds van belang is.
Bij de parlementaire behandeling van het meergenoemde voorstel is naar voren gekomen dat zowel de regering als de Tweede Kamer e-mail onder de bescherming van artikel 13 wil brengen. Bijzondere beveiligingsvormen (encryptie) zijn daarbij in beginsel niet vereist. In de systematiek van artikel 13 is e-mail het meest vergelijkbaar met telefoon, maar

vertoont het ook een overeenkomst met een brief, 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, dan ook onder de grondwettelijke bescherming vallen. Aangenomen moet worden dat de bescherming van e-mail onafhankelijk is van het gebruikte transportmiddel (gewone telefoonlijn, ISDN, radio- en televisiekabel).
Mede gelet op de discussie rond het genoemde voorstel tot wijziging van de Grondwet ben ik van mening dat elektronische post in het strafrecht in dezelfde mate beschermd dient te worden als een brief of een telefoongesprek. Met de hiervoor noodzakelijke wetswijziging wil de regering niet wachten tot een eventueel nieuw voorstel tot wijziging van artikel 13 Grondwet in werking zal zijn getreden, omdat de behoefte aan wettelijke bescherming van e-mail nu al wordt gevoeld. De Vereniging van Nederlandse Internet Providers (NLIP) heeft in haar commentaar opgemerkt van «harte in te stemmen» met wettelijke bescherming van e-mail. De NVvR spreekt van «een logisch gevolg van de toegenomen betekenis van elektronisch gegevensverkeer.» Hierbij dient te worden aangetekend dat e-mail slechts een bijzondere strafrechtelijke bescherming verdient voor zover de afzender de van buitenaf kenbare wil heeft om het bericht vertrouwelijk te houden. Persoonlijk geadresseerde e-mail is evenals de brief niet bestemd om te worden gelezen door anderen en verdient uit dien hoofde bescherming. De wil tot vertrouwelijkheid blijkt ook in dit geval uit de aard van de toegepaste techniek. Zelfs indien iemand zich zonder toestemming van de geadresseerde de toegang kan verschaffen tot de mailbox van een ander – dat is niet eenvoudig gelet op de gangbare beveiliging met een password[4] – is het gelet op de bij e-mail toegepaste software niet goed mogelijk de ongelezen e-mail van die ander te lezen zonder dat die daarvan achteraf op de hoogte geraakt. Na lezing zal het desbetreffende bericht immers automatisch in de map «gelezen» of iets dergelijks terechtkomen, waardoor de geadresseerde achteraf kan vaststellen dat onbevoegd kennis is genomen van zijn ongelezen e-mail. De vergelijking met de opengescheurde envelop is hier op zijn plaats. In beide gevallen heeft de verzender door de keuze van het communicatiemiddel voorzien in een voorzorgsmaatregel met betrekking tot de vertrouwelijkheid van zijn bericht dat in ieder geval zo ver strekt dat de geadresseerde van eventuele onbevoegde lezing doorgaans achteraf kennis zal kunnen nemen. Hierin ligt een essentieel verschil met de briefkaart. Noch met betrekking tot persoonlijk geadresseerde e-mail noch met betrekking tot gesloten brieven is dus sprake van een absolute onmogelijkheid tot onbevoegde kennisneming door derden. De wil tot vertrouwelijkheid hoeft ook niet uit een absolute onmogelijkheid tot de schending van dat vertrouwen te blijken – in het laatste geval zou strafrechtelijke bescherming niet noodzakelijk zijn –, doch dient te blijken uit het feit dat een communicatiemiddel wordt toegepast dat in beginsel besloten is en op grond van de in het maatschappelijk verkeer geldende opvattingen ook zo behoort te blijven. Persoonlijk geadresseerde e-mail dient op grond van hetgeen hierboven uiteen is gezet zonder meer als zodanig te gelden. Wie daarentegen een e-mail verzendt naar een openbare nieuwsgroep of een openbaar bulletin-board en weet of kan weten dat zijn bericht voor een ieder is in te zien, heeft niet de (geobjectiveerde) wil om het bericht vertrouwelijk te houden en heeft dus géén aanspraak op vertrouwelijkheid. Het voorgaande heeft uiteraard uitsluitend betrekking op de fase van opslag van e-mail. Voor wat betreft de transportfase van e-mail over een telecommunicatienetwerk dient opgemerkt te worden dat deze geheel gelijkwaardig is aan de transportfase van telefoonverkeer en uit dien hoofde dezelfde grondwettelijke bescherming zal dienen te genieten.

[4] In de kamerstukken met betrekking tot het verklaringsvoorstel tot verandering in de Grondwet van de bepalingen inzake de onschendbaarheid van het brief-, telefoon-, en telegraafgeheim, waarin door de regering aanvankelijk een algemeen, techniek-onafhankelijk recht op vertrouwelijke communicatie werd geïntroduceerd, was als uitgangspunt genomen dat waar het e-mail betrof de beveiliging met een password een noodzakelijke voorwaarde was voor de wil tot vertrouwelijkheid (Kamerstukken II 1997/98, 25 443, nr. 5). Het door de Tweede Kamer geamendeerde verklaringsvoorstel, waarin de bescherming van de bestaande communicatie-technieken gehandhaafd werd en uitgebreid werd naar andere vergelijkbare technieken, noopte tot een interpretatie van de grondwettelijke bescherming van e-mail, die meer via analogie moest worden afgeleid uit de bescherming die aan brief en telefoon toekomt.

In deze paragraaf wordt nagegaan in hoeverre het huidige recht reeds bescherming biedt aan e-mail en welke aanpassingen eventueel wenselijk zijn. Hierbij wordt onderscheid gemaakt tussen de fase van opslag van e-mail op een computer en de fase van het transport van e-mail over een telecommunicatienetwerk. Voorts wordt onderscheiden tussen het materiële strafrecht (de strafbare handelingen) en het formele strafrecht (strafvorderlijke bevoegdheden).
Wat de fase van het *transport* betreft is de bescherming van e-mail reeds nagenoeg compleet. Materieelrechtelijk geldt het in artikel 139c Sr gesanctioneerde verbod om voor een ander bestemde gegevens die via openbare telecommunicatienetwerken worden overgedragen, met een technisch hulpmiddel af te tappen of op te nemen. Dit verbod geldt natuurlijk ook voor e-mail via bijvoorbeeld Internet. Ook voor zover e-mail in besloten kring wordt verzonden – bijvoorbeeld via een intern bedrijfsnetwerk – zijn bestaande aftapverboden van toepassing (zie artikelen 139a en 139b, telkens het tweede lid, Sr). Daarnaast geldt een bijzonder aftapverbod voor personen die belast zijn met de «dienst ten behoeve van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst» (artikel 374bis Sr zoals gewijzigd bij de nieuwe Telecommunicatiewet; artikel 374bis wordt in dit wetsvoorstel vernummerd tot artikel 273d Sr). Deze strafbepaling wordt gerechtvaardigd door de plicht die op deze personen rust, om ervoor te zorgen dat gegevens, overgedragen via telecommunicatie, ongeschonden overkomen zonder dat onbevoegden ervan kunnen kennisnemen. Bovendien kan de gelegenheid die hun functie hun biedt, hen in de verleiding brengen om zelf van voor anderen bestemde gegevens kennis te nemen. Met de nieuwe Telecommunicatiewet strekt deze strafbepaling zich uit tot iedere persoon werkzaam bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst. Daarmee vallen ook werknemers van bijvoorbeeld Internet Service Providers onder het bijzondere aftapverbod.
Aan de strafvorderlijke kant gelden ten aanzien van e-mail (in transport) de normale bepalingen betreffende het aftappen en opnemen van telecommunicatie via openbare telecommunicatienetwerken (zie het huidige artikel 125g Sv en de artikelen 126m en 126t volgens de Wet bijzondere opsporingsbevoegdheden). Als justitie ten behoeve van de waarheidsvinding het e-mailverkeer van en naar een bepaalde persoon wil opnemen, zal dat dus op basis van deze bepalingen moeten geschieden (zie ook paragraaf 5.2 over de functionele betekenis van «opnemen van telecommunicatie»). Hieraan worden dezelfde eisen gesteld als aan het aftappen van een traditioneel telefoongesprek. Met de nieuwe Telecommunicatiewet zijn ook Internet Service Providers verplicht hun medewerking te verlenen aan het aftappen van e-mail door justitie.
Wat betreft e-mail die *is opgeslagen* in een computer geldt de algemene bescherming die de strafwet geeft aan geautomatiseerde werken: het is verboden wederrechtelijk binnen te dringen in een geautomatiseerd werk, of in een deel daarvan, met doorbreking van enige beveiliging of door een technische ingreep, met behulp van valse signalen of een valse sleutel of door aanneming van een valse hoedanigheid (computervredebreuk, artikel 138a, eerste lid, Sr). Ingevolge artikel 138a, tweede lid, is een hoger strafmaximum (maximaal 4 jaren gevangenisstraf of geldboete van de vierde categorie) van toepassing indien de dader gegevens die zijn opgeslagen in het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt. Zoals aangegeven in paragraaf 5.2 wordt dit tweede lid overigens uitgebreid tot het, eenmaal in de computer zijnde, aftappen of opnemen van stromende gegevens, waarmee artikel 138a lid 2 dus ook bescherming verleent aan e-mail in transport.
Artikel 138a Sr geeft primair bescherming aan (delen van) geautomatiseerde werken. De bescherming van de daarin aanwezige gegevens is

daarvan een afgeleide. Daarbij maakt het niet uit om wat voor soort gegevens het gaat; zowel e-mailberichten als een adressenbestand genieten bescherming (vgl. de diefstalbepalingen, waarbij het ook niet uitmaakt of de diefstal een TV-toestel betreft of een brief). Onder «een deel» van een geautomatiseerd werk in de zin van artikel 138a Sr kan bijvoorbeeld worden verstaan de voor een bepaalde persoon gereserveerde ruimte op de harde schijf van een netwerkserver. Deze ruimte moet wel op een of andere wijze zijn afgeschermd (bijvoorbeeld door middel van een password), zodat onbevoegden haar niet zonder meer kunnen betreden. Hier wordt dus wel enige vorm van beveiliging van computergegevens (althans van de computer waarin zich die gegevens bevinden) geëist, in tegenstelling tot bijvoorbeeld de hiervoor besproken situatie dat gegevens over een telecommunicatienetwerk worden verzonden: in dat geval kan zoals gezegd uit de adressering aan bepaalde personen reeds een aanspraak op bescherming volgen. Ik meen dat dit verschil wordt gerechtvaardigd door het feit dat de bescherming van artikel 138a Sr is bedoeld voor personen die een computer onder hun beheer hebben of over een deel daarvan kunnen beschikken. Deze personen hebben het in het algemeen in hun macht die computer of dat deel al dan niet te beveiligen. Wie daarentegen gegevens over een telecommunicatienetwerk verzendt, heeft die macht niet of in veel mindere mate en is mede afhankelijk van de telecommunicatieaanbieder en de zorg die deze betracht.

Op één punt schiet de materieelstrafrechtelijke bescherming van opgeslagen e-mail mogelijk tekort. Het is namelijk twijfelachtig of een Internet Service Provider zich schuldig maakt aan computervredebreuk als hij zonder de toestemming van een abonnee in diens mailbox kijkt. Aangezien die mailboxen zich op een geautomatiseerd werk bevinden dat eigendom is van de provider, is het immers de vraag of gesproken kan worden van *wederrechtelijk* binnendringen in het geautomatiseerd werk door de provider. Dit neemt mijns inziens niet weg dat telecommunicatieaanbieders, gelet op de bijzondere zorgplicht die zoals gezegd op hen rust, niet gerechtigd zijn kennis te nemen van niet voor hen bestemde gegevens die in hun computers zijn opgeslagen. Om deze reden wordt voorgesteld – conform de toezegging gedaan in de nota naar aanleiding van het verslag bij (het inmiddels ingetrokken) wetsvoorstel 25 443 tot wijziging van artikel 13 Grondwet – om de strafbaarstelling die thans is vervat in artikel 374bis Sr en ziet op het wederrechtelijk aftappen van telecommunicatie door een persoon werkzaam bij een telecommunicatieaanbieder, uit te breiden tot het door een dergelijke persoon wederrechtelijk kennisnemen of overnemen van niet voor hem bestemde gegevens die zijn opgeslagen in de computers van die operator (zie het voorgestelde artikel 273d Sr). Aanvankelijk was de beoogde strafbaarstelling opgenomen in een nieuw tweede lid in artikel 372 Sr, dat kortweg ziet op de postbode die een hem toevertrouwde brief wederrechtelijk opent. Terecht merkte de Registratiekamer op dat door deze plaatsing (en de in verband daarmee gehanteerde terminologie) de verhouding tot artikel 374bis en de aftapverboden van de artikelen 139a tot en met 139c Sr onduidelijk was. Door de aansluiting bij artikel 374bis (het nieuwe 273d Sr) is de onderlinge verhouding en samenhang tussen de artikelen duidelijker.

Over de mogelijkheden voor justitie om e-mail die is opgeslagen in een geautomatiseerd werk, ten behoeve van de strafvordering te vergaren en in te zien merk ik het volgende op. De twee meest gebruikelijke, tot dit doel openstaande wegen zijn die van een vordering van de rechter-commissaris op grond van artikel 125i, eerste lid, Sv en die van de huiszoeking waarbij de ter plaatse aanwezige computers worden onderzocht. Zoals in paragraaf 5.2 aangegeven dient de bevoegdheid van artikel 125i zoals gewijzigd bij dit wetsvoorstel uitsluitend nog tot het verkrijgen van gegevens die ten tijde van het bevel van de RC reeds zijn

opgeslagen in een computer. Ook de huiszoekingsbevoegdheid strekt alleen tot het onderzoek in geautomatiseerde werken naar bestaande, in zo'n werk opgeslagen gegevens.
Zowel artikel 125i, eerste lid, als artikel 125j, eerste lid, ziet op alle computergegevens. Zij stellen geen extra eisen aan het onderzoek van bijvoorbeeld e-mail. Op grond van een vergelijking met de regeling van de inbeslagneming van (stoffelijke) geschriften ben ik van oordeel dat die er wel moeten komen. In die regeling is namelijk voorzien in een bijzondere positie voor brieven en andere post voor zover ze zijn toevertrouwd aan een *instelling van vervoer*. Art. 100 Sv (zoals voorzien bij de Wet herziening van het gerechtelijk vooronderzoek)[5] bepaalt dat de officier van justitie instellingen van vervoer kan bevelen poststukken uit te leveren alleen voor zover zij *klaarblijkelijk* van de verdachte afkomstig zijn, voor hem bestemd zijn of op hem betrekking hebben, ofwel indien zij klaarblijkelijk het voorwerp van het strafbare feit uitmaken of tot het begaan daarvan gediend hebben. De artikelen 101, tweede lid, en 114, tweede lid, bepalen vervolgens dat van de inhoud van inbeslaggenomen poststukken, voor zover ze gesloten zijn, alleen wordt kennisgenomen met toestemming van de rechter-commissaris en alleen voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd enz. Voor het verkrijgen van inzage door justitie in post die berust onder een vervoersinstelling, gelden dus zwaardere eisen dan voor het onderzoek van voorwerpen en geschriften in het algemeen; met name dient een hogere graad van waarschijnlijkheid («klaarblijkelijk») te bestaan dat de gezochte gegevens direct relevant zijn voor het onderzoek. Doel van deze eisen is om een extra waarborg te geven voor de vertrouwelijkheid van het postvervoer zoals dat wordt verzorgd door professionele vervoersinstellingen.
Ik ben van mening dat het gewenst is de eisen die gelden voor het onderzoek van poststukken die zich onder een vervoersinstelling bevinden, door te trekken naar het justitieel onderzoek van e-mail voor zover die is opgeslagen bij de desbetreffende «vervoersinstellingen» (dat wil zeggen ISP's). Daarmee wordt tevens aangesloten bij de strekking van artikel 13 Grondwet: voor de bescherming van opgeslagen e-mail wordt aangesloten bij het grondwettelijke postgeheim, nu zowel e-mail als post vormen van uitgestelde communicatie zijn. Concreet houdt het voorstel in dat gegevens die zijn opgeslagen op de computer van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst en die niet voor deze bestemd of van deze afkomstig zijn, door justitie slechts kunnen worden ingezien op bevel van de rechter-commissaris en alleen voor zover die e-mails klaarblijkelijk van de verdachte afkomstig zijn, voor hem zijn bestemd of tot het begaan van het strafbare feit hebben gediend, ofwel klaarblijkelijk met betrekking tot die e-mails het strafbare feit is gepleegd. Zie de voorgestelde artikelen 125i, derde lid, en 125n Sv. De term «klaarblijkelijk» betekent in dit verband dat alleen van die gegevens kan worden kennisgenomen waarvan van buitenaf (bijvoorbeeld op grond van de adressering of de herkomstgegevens van het bericht), eventueel mede gelet op andere uit het onderzoek bekende gegevens, duidelijk is dat ze van de verdachte afkomstig zijn, voor hem bestemd enz. Politie, officier van justitie of RC zijn uiteraard niet bevoegd om aangetroffen e-mails eerst in te zien om te kijken of ze voldoen aan de criteria van de artikelen 125i en 125n. Artikel 125n Sv ziet op de situatie dat bij onderzoek in het geautomatiseerd werk van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst (bijvoorbeeld ter gelegenheid van een huiszoeking) gegevens worden aangetroffen die niet voor deze bestemd of van deze afkomstig zijn.

In onderstaande tabel is de strafrechtelijke bescherming van e-mail zoals die na invoering van de onderhavige voorstellen zal zijn geregeld, samengevat.

[5] De wet van 27 mei 1999 tot partiële wijziging van het Wetboek van Strafvordering (herziening van het gerechtelijk vooronderzoek) (Stb. 243), nog niet in werking getreden.

| bescherming van e-mail | in transport | opgeslagen e-mail |
|---|---|---|
| materieel strafrecht | 138a.1jo.2 Sr (aftappen na computervredebreuk)<br>139c Sr (aftappen openbare telecom)<br>139a.2, 139b.2 (aftappen besloten gegevensoverdracht)<br>273d (374bis oud) (aftappen door werknemers van telecommunicatieaanbieders) | 138a.1jo.2 Sr (kopiëren opgeslagen gegevens na computervredebreuk)<br>273d (kennisnemen en overnemen door werknemers telecommunicatieaanbieders van niet voor hen bestemde gegevens) |
| strafprocesrecht | 126m, 126t (125g oud) Sv (opnemen van telecommunicatie) | 125i.1jo.3 Sv (vordering van gegevens opgeslagen bij telecommunicatieaanbieders)<br>125n (kennisnemen van gegevens aangetroffen bij telecommunicatieaanbieders) |

## 7. Opsporingsonderzoek op openbare computernetwerken

*7.1 Inleiding*

Met de opkomst van openbare computernetwerken zoals Internet is de vraag actueel geworden wat opsporingsambtenaren op deze netwerken vermogen. In het bijzonder rijst de vraag of de bestaande opsporingsbevoegdheden alsmede de bij de Wet bijzondere opsporingsbevoegdheden voorziene bevoegdheden op Internet kunnen en mogen worden uitgeoefend, dan wel aanpassing behoeven.
Onderscheid dient te worden gemaakt tussen het rondkijken op een netwerk voor zover dat voor het publiek toegankelijk is en het verrichten van (opsporings)handelingen op zo'n netwerk waarbij inbreuk wordt gemaakt op de (grond)rechten van burgers. Wat het eerste betreft staat niets de politie in de weg om een contract te sluiten met een provider teneinde een aansluiting te verkrijgen op Internet. Vervolgens kunnen politie-ambtenaren als ieder ander rondkijken in de digitale wereld en kennis nemen van de voor een ieder raadpleegbare informatie. Daarvoor is niet vereist dat zij een verdenking van een strafbaar feit hebben. Evenmin behoeven zij hun hoedanigheid van opsporingsambtenaar bekend te maken. Zoals de politie, al dan niet in burger, op straat mag surveilleren en rondkijken, zo mag een rechercheur vanachter zijn computer hetzelfde doen op Internet. Een uitdrukkelijke wettelijke grondslag is daarvoor niet nodig, mits dat optreden gerekend kan worden tot de uitvoering van de politietaak (zie artikel 2 Politiewet 1993).
Een en ander geldt mijns inziens ook voor Internetsites die aan opsporingsambtenaren de toegang ontzeggen («Stop! Are you a law enforcement agent?»). Beheerders van dergelijke sites kunnen redelijkerwijs niet de verwachting hebben dat, waar zo'n site voor ieder ander toegankelijk is en dus feitelijk een openbaar karakter draagt, alleen opsporingsambtenaren zich van kennisneming zullen onthouden. Opsporingsambtenaren behoeven zich in zo'n geval dan ook niet aan het toegangsverbod te storen. Evenmin behoeven zij zich onder hun werkelijke naam of hoedanigheid bekend te maken wanneer zij bijvoorbeeld eenmalig in een openbare nieuwsgroep een bericht posten. Het is immers op veel delen van Internet niet ongebruikelijk om je daar anoniem of onder een pseudoniem te bewegen. De overige deelnemers kunnen er in die gevallen op bedacht zijn dat ze in werkelijkheid met iemand anders van doen hebben. Alleen wanneer het onder pseudoniem opereren van een opsporingsambtenaar als misleiding van andere gebruikers van Internet moet worden aangemerkt (bijvoorbeeld in bepaalde wetenschappelijke nieuwsgroepen waarin dat als onfatsoenlijk wordt beschouwd), moet het hanteren van een pseudoniem door een opsporingsambtenaar in het

algemeen ongeoorloofd worden geacht. Verder geldt dat wanneer het onderzoek een stelselmatig karakter krijgt, het een aparte juridische legitimatie behoeft (zie de volgende paragraaf).
De bevoegdheid om rond te kijken op een openbaar netwerk impliceert nog niet de bevoegdheid om stelselmatig voor de uitoefening van de politietaak gegevens omtrent onverdachte personen van Internet te downloaden en in een politieregister op te slaan. Dergelijke gegevens mogen blijkens artikel 4 van de Wet politieregisters immers slechts worden opgeslagen voor zover dat noodzakelijk is voor de uitoefening van de politietaak. Dit laat onverlet dat voor de opsporing van een bepaald strafbaar feit uiteenlopende persoonsgegevens van Internet worden gedownload en worden opgenomen in een tijdelijk register in de zin van deze wet, teneinde vervolgens te kunnen worden geanalyseerd en in verband gebracht met andere gegevens.
Tegenover het rondkijken op een openbaar netwerk staat het op zo'n netwerk verrichten van opsporingshandelingen waarbij inbreuk wordt gemaakt op de rechten van burgers. Daartoe zijn politie en justitie alleen bevoegd indien daarvoor een uitdrukkelijke wettelijke grondslag bestaat. Veel van de bestaande wettelijke opsporingsbevoegdheden zijn op een computernetwerk naar hun aard niet toepasbaar omdat toepassing alleen aan de orde kan zijn bij de fysieke aanwezigheid van personen of goederen, zoals de aanhouding van verdachten of de inbeslagneming van voorwerpen. Andere bevoegdheden daarentegen kunnen op een netwerk wel degelijk relevant zijn. Ik wijs op de in dit wetsvoorstel voorgestelde bevoegdheden tot ontoegankelijkmaking en vernietiging van bepaalde gegevens – de desbetreffende bepalingen maken geen onderscheid tussen een stand alone computer en een computer die is verbonden met een netwerk, zodat ze ook op een netwerk toepasbaar zijn –, alsmede op bijzondere opsporingsbevoegdheden zoals infiltratie en observatie, die thans nog op ongeschreven recht zijn gebaseerd maar door de Wet bijzondere opsporingsbevoegdheden van een wettelijke basis worden voorzien. Uitgangspunt bij dit soort bevoegdheden (die dus niet noodzakelijk betrekking hebben op fysiek aanwezige personen of goederen) dient mijns inziens te zijn dat ze, naast de «normale» toepassing in de fysieke wereld, ook toepasbaar moeten zijn in de «digitale wereld». Daarbij dienen dezelfde voorwaarden te gelden als voor de normale toepassing, tenzij de specifieke aard van het onderzoek in een geautomatiseerde omgeving om specifieke voorzieningen vraagt. In de volgende paragraaf zullen enkele bijzondere opsporingsbevoegdheden aan dit uitgangspunt worden getoetst.
Bij het voorgaande dient een belangrijk voorbehoud te worden gemaakt. Nederlandse opsporingsambtenaren mogen 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 lijdt voor zover de opsporingsambtenaar, zoals hierboven aangegeven, als ieder ander mag rondkijken op een openbaar netwerk. Het staat een opsporingsambtenaar dus vrij om met sites waarvan de databestanden zijn opgeslagen op buitenlandse computers, een verbinding te leggen teneinde die sites te bekijken. Wat de opsporingsambtenaar echter níet mag, is op die sites bevoegdheden uitoefenen waarbij inbreuk wordt gemaakt op de rechten van burgers. Voor de voorgestelde maatregel van ontoegankelijkmaking van gegevens betekent dit bijvoorbeeld dat hij niet mag worden toegepast ten aanzien van gegevens waarvan men redelijkerwijs kan vermoeden dat zij zijn opgeslagen in een buitenlandse computer en zich dus aan de Nederlandse rechtsmacht onttrekken. Indien de maatregel op goede gronden wordt toegepast, maar later blijkt dat, anders dan redelijkerwijs kon worden vermoed, de maatregel *de facto* in een computer in het

buitenland heeft plaatsgevonden, moet onmiddellijk contact worden opgenomen met de autoriteit van het desbetreffende land teneinde in onderling overleg te bezien wat te doen staat.
Overigens zijn grensoverschrijdende opsporingshandelingen wel toegelaten indien ze een basis vinden in het volkenrecht of het interregionale recht (vgl. art. 539a, derde lid, Sv). Daarbij moet allereerst worden gedacht aan een basis in een verdrag. In hoeverre de enkele toestemming van de autoriteiten van een vreemde staat, zonder verdragsrechtelijke grondslag, grensoverschrijdende handelingen van Nederlandse opsporingsambtenaren kan legitimeren, is onduidelijk. Zoals in paragraaf 1 al aangegeven is in het kader van de Raad van Europa een verdrag in voorbereiding, waarin dit soort rechtsmachtkwesties centraal staan.

*7.2 Bijzondere opsporingsbevoegdheden; pseudokoop*

In de memorie van toelichting bij het wetsvoorstel dat heeft geleid tot de Wet bijzondere opsporingsbevoegdheden (kamerstukken II 1996/97, 25 403, nr. 3) wordt op verschillende plaatsen ingegaan op de toepasbaarheid van de voorgestelde bevoegdheden op een openbaar computernetwerk zoals Internet. Zo is daarin aangegeven dat infiltratie – het door een opsporingsambtenaar deelnemen of medewerking verlenen aan een groep van personen waarbinnen naar redelijkerwijs kan worden vermoed misdrijven worden beraamd of gepleegd (zie de artikelen 126h en 126p Sv) – ook mogelijk is op Internet (memorie van toelichting, a.w., p. 29). Daarbij is als voorbeeld gegeven de infiltratie in een netwerk van personen dat via Internet kinderporno distribueert, waarbij de opsporingsambtenaar zich (ook) op het net dient te begeven. Kenmerkend voor infiltratie is dat wordt meegewerkt of deelgenomen aan een criminele groep, zodat het risico bestaat dat de betrokken opsporingsambtenaar strafbare feiten moet plegen, terwijl de andere deelnemers worden misleid omtrent de werkelijke motieven van de infiltrant. Gelet op dit (ingrijpende) karakter is de bevoegdheid aan strikte voorwaarden gebonden (onder andere is een bevel van de officier van justitie vereist). Aan deze voorwaarden zal ook bij optreden op Internet moeten worden voldaan.
Mutatis mutandis geldt hetzelfde voor het zogenaamd stelselmatig inwinnen van informatie over de verdachte, zonder dat de opsporingsambtenaar als zodanig kenbaar is (zie artikel 126j Sv). Denkbaar is dat dit de vorm aanneemt van het stelselmatig inwinnen van informatie in een nieuwsgroep op Internet waaraan ook de verdachte deelneemt, zonder dat de deelnemers aan de nieuwsgroep weten dat zich onder hen een opsporingsambtenaar bevindt (memorie van toelichting, a.w., p. 34). Hierbij gaat het overigens alleen om het door de ambtenaar *actief* deelnemen aan de nieuwsgroep, doordat hij of zij zelf berichten post en aldus tracht van anderen informatie los te krijgen; het slechts rondkijken in een nieuwsgroep en lezen wat voor een ieder toegankelijk is, is zoals eerder aangegeven zonder meer geoorloofd. De bevoegdheid tot het stelselmatig inwinnen van informatie over de verdachte onderscheidt zich van infiltratie doordat niet wordt deelgenomen aan een groep van personen waarbinnen misdrijven worden beraamd of gepleegd. Kenmerkend is verder dat sprake is van een stelselmatig onderzoek; alleen in geval van stelselmatigheid kan worden gesproken van een zodanige inbreuk op de persoonlijke levenssfeer van de verdachte dat het onderzoek aan de voorwaarden van artikel 126j moet voldoen.
Een andere bevoegdheid uit de Wet bijzondere opsporingsbevoegdheden blijkt niet geschikt voor toepassing op een computernetwerk, terwijl dit wel wenselijk is. Het betreft de bevoegdheid tot pseudo-koop en pseudodienstverlening, dat wil zeggen het in het belang van het onderzoek door een opsporingsambtenaar goederen afnemen van of diensten verlenen aan de verdachte (zie de artikelen 126i en 126q Sv). Hierbij is met name

gedacht aan fysieke handelingen zoals het afnemen van drugs en het verlenen van transportdiensten. Op Internet zijn echter opsporingshandelingen denkbaar die erg op de genoemde lijken en dezelfde strekking hebben, maar niettemin niet onder de thans voorgestelde bepalingen kunnen worden gebracht. Ik doel hier op onderzoek naar de handel op Internet in illegale uitingen of programmatuur (bijvoorbeeld illegale software, kinderporno). Het kan daarbij wenselijk zijn dat een politie-ambtenaar op een bepaalde aanbieding ingaat en de betrokken gegevens afneemt. In de praktijk is gebleken dat aan een daartoe strekkende bevoegdheid behoefte bestaat. Ook het in de vorige paragraaf genoemde uitgangspunt dat wat in de fysieke wereld ter opsporing mogelijk is, in de digitale wereld ook mogelijk moet zijn, rechtvaardigt een aanpassing van de pseudekoopbepalingen. Ik stel dan ook voor in de bij de Wet bijzondere opsporingsbevoegdheden voorziene artikelen 126i en 126q op te nemen dat de officier van justitie in het belang van het onderzoek kan bevelen dat een opsporingsambtenaar *«gegevens die zijn opgeslagenopgeslagen, worden verwerkt of overgedragen door middel van een geautomatiseerd werk, door tussenkomst van een openbaar telecommunicatienetwerk afneemt van de verdachte»*. Het «afnemen» van gegevens via bijvoorbeeld Internet veronderstelt overigens wel een direct contact, althans een directe relatie tussen de verdachte en een opsporingsambtenaar, waardoor de eerste wordt bewogen bepaald (bijvoorbeeld strafbaar) materiaal aan de laatste te leveren. Doorgaans zal daar een tegenprestatie – in de vorm van een ruil of betaling – tegenover staan. Onder afnemen van gegevens valt dus niet de situatie waarin op Internet aanwezig materiaal (bijvoorbeeld kinderporno) dat beschikbaar is voor eenieder die het maar wil hebben, door een opsporingsambtenaar wordt gedownload; hiervoor is geen expliciete wettelijke grondslag nodig. Terecht wijst de Registratiekamer er in zijn advies op dat de voorgestelde bevoegdheid op zichzelf slechts gebruikt kan worden in de publiek toegankelijke digitale wereld en niet legitimeert tot het «betreden» van besloten plaatsen of het kennisnemen van besloten processen. Ik voeg er echter aan toe dat andere bevoegdheden zoals de hiervoor genoemde bevoegdheden tot infiltratie en het stelselmatig inwinnen van informatie het mogelijk maken om in de nabijheid van een verdachte te komen. Vervolgens kan de pseudokoopbevoegdheid worden uitgeoefend.
In de Wet bijzondere opsporingsbevoegdheden is ook de zogenaamd burgerpseudo-koop geregeld, dat wil zeggen de bijstandverlening aan de opsporing door een gewone burger bestaande uit het door deze afnemen van goederen van of het verlenen van diensten aan de verdachte (artikelen 126ij en 126z Sv). Ik heb ervan afgezien om ook deze bepalingen aan te passen aan de opsporing in een openbaar computernetwerk, aangezien de tussenkomst van een netwerk het de politie mogelijk maakt om de pseudokoop altijd zelf uit te voeren.

## 8. Overige wijzigingen

In deze paragraaf worden enkele min of meer principiële voorstellen besproken die in het voorgaande geen plaats konden krijgen.

*a. Schending van het brief-, telefoon- en telegraafgeheim*

De huidige artikelen 372 tot en met 375 van het Wetboek van Strafrecht bevatten strafbaarstellingen van ambtenaren die zich schuldig maken aan schending van het brief-, telefoon- of telegraafgeheim. Bij de wet van 26 oktober 1988, Stb. 521, werden de strafbaarstellingen van de ambtenaren van de post in verband met de privatisering van de PTT uitgebreid tot «een persoon werkzaam bij enige openbare instelling van vervoer». Ondanks de privatisering werd handhaving bij de ambtsdelicten gerechtvaardigd geacht vanwege de publieke nutsfunctie van de postale dienst-

verlening. Inmiddels is bij de nieuwe Telecommunicatiewet artikel 374bis Sr gewijzigd in verband met de liberalisering van de telecommunicatiemarkt; dit artikel richt zich nu onder andere tot een persoon belast met de dienst ten behoeve van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst. Bij deze stand van zaken en mede gelet op de voor de komende jaren in EG-verband voorgenomen liberalisering van de postmarkt ben ik van mening dat de band van de artikelen 372 tot en met 375 Sr met de «echte» ambtsdelicten een nogal onrechtstreekse is geworden en dat handhaving bij de ambtsdelicten niet meer voor de hand ligt. Nu ik, zoals reeds aangegeven in paragraaf 6.2, ook anderszins voorstel om m.n. artikel 374bis Sr terminologisch te wijzigen, wil ik dan ook van de gelegenheid gebruikmaken om de bepalingen betreffende schending van het brief-, telefoon- en telegraafgeheim uit titel XXVIII te halen en over te hevelen naar titel XVII van boek 2 betreffende «schending van geheimen». Plaatsing in die titel geeft goed aan dat het accent is komen te liggen op de schending van het communicatiegeheim door personen die gelet op hun functie een bijzondere verantwoordelijkheid hebben ten aanzien van de bescherming van dat geheim.
Bij de overheveling van de onderhavige bepalingen naar de nieuwe artikelen 273a tot en met 273e Sr zijn overigens, afgezien van artikel 273d Sr (artikel 374bis oud), zo min mogelijk wijzigingen aangebracht. De «ambtenaar» is daaruit uiteraard verdwenen, evenals de in de artikelen 374 en 374bis nog genoemde toezichthouders. Bij deze laatsten moet men denken aan ambtenaren van het Ministerie van Verkeer en Waterstaat en van de OPTA (Onafhankelijke post- en telecommunicatieautoriteit), op wie het bestaande artikel 272 Sr reeds van toepassing is. De aparte strafbepaling voor schending van het telegraafgeheim blijft vooralsnog gehandhaafd (artikel 374 oud, artikel 273c nieuw), ondanks het meer en meer in onbruik raken van de telegrafie en de convergentie met andere vormen van telecommunicatie. Op grond van het Internationaal Telecommunicatieverdrag (ITU) is Nederland echter verplicht een dergelijke dienst in stand te houden.

*b. Strafbepalingen ter bescherming van het functioneren van informatiesystemen*

In de huidige tijd is het goed functioneren van informatiesystemen belangrijker dan ooit. Het strafrecht kan daarbij een beschermende rol vervullen door de strafbaarstelling van wat wel wordt genoemd CIA-delicten, dat wil zeggen handelingen waardoor de *confidentiality* (vertrouwelijkheid van gegevens), de *integrity* (integriteit van systemen) of de *availability* (ongestoorde beschikbaarheid van gegevens, programmatuur en diensten) van gegevens en de desbetreffende systemen worden aangetast. In de nota «Wetgeving voor de elektronische snelweg» zijn daarover enkele opmerkingen gemaakt (kamerstukken II 1997/98, 25 880, nrs. 1–2, blz. 76/77). Ter bescherming van informatiesystemen bevat het onderhavige wetsvoorstel de volgende wijzigingen en aanvullingen van het Wetboek van Strafrecht.
De artikelen 350a en 350b Sr stellen thans strafbaar het (opzettelijk respectievelijk culpoos) veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen. Bij de totstandkoming van deze bepalingen (bij de eerste Wet computercriminaliteit) zal primair zijn gedacht aan de gegevensverwerking binnen één computer – met name aan daarin opgeslagen gegevens – en niet zozeer aan het «vernielen» van gegevens die door middel van computernetwerken worden overgedragen. Nu inmiddels gegevensoverdracht via computernetwerken een grote vlucht heeft genomen en het (wederrechtelijk) wijzigen van dergelijke «stromende» gegevens technisch mogelijk is, is het mijns inziens wenselijk om buiten twijfel te stellen dat de artikelen

350a en 350b Sr ook strekken tot bescherming van de integriteit van gegevensverwerking of -overdracht tussen computers. Daartoe wordt voorgesteld expliciet strafbaar te stellen het vernielen van gegevens die door middel van een geautomatiseerd werk *of door middel van telecommunicatie* worden verwerkt of overgedragen. Dit is in overeenstemming met een aanbeveling in de genoemde nota.
*Spam* – het ongevraagd toezenden van e-mail, waarbij de afzender vaak een onjuist adres opgeeft zodat de ontvanger geen actie tegen hem kan ondernemen – wordt op Internet in toenemende mate als een probleem ervaren. De Vereniging van Nederlandse Internet Providers (NLIP) heeft in haar commentaar op het ontwerp van dit wetsvoorstel gepleit voor een betere formulering en strafbaarstelling van spam. Ook de Beleidsadviesgroep digitaal rechercheren van de politie heeft aandacht gevraagd voor deze «digitale variant van stalking». Onder spam worden verschillende gedragingen verstaan met verschillende gevolgen. De «klassieke» vorm is het ongevraagd toezenden van een e-mail aan een groot aantal personen. Vaak gebeurt dit voor reclamedoeleinden (direct marketing). Daarnaast is er het toezenden van een grote hoeveelheid e-mail (inhoud vaak niet relevant, bijvoorbeeld tienmaal de bijbel) aan één persoon met als doel dat diens e-mailbox verstopt raakt waardoor hij geen e-mails meer kan ontvangen. Dit wordt ook wel bombing genoemd. In zo'n geval is de beschikbaarheid (availability) van een Internetdienst voor individuele gebruikers in het geding. Dergelijke bombardementen van e-mails kunnen dusdanig ernstige vormen aannemen dat zelfs de werking van de server van een Internet Service Provider tijdelijk wordt verstoord en daardoor diens dienstverlening ernstig wordt bemoeilijkt. In zo'n geval kan sprake zijn van het strafbaar feit van artikel 161sexies (onderdeel 1) of artikel 161septies (onderdeel 1) Sr: het (opzettelijk dan wel culpoos) vernielen, beschadigen, onbruikbaar maken, stoornis in de werking veroorzaken enz., van een geautomatiseerd werk, waardoor wederrechtelijk verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst ontstaat.
Ik meen, mede gelet op de genoemde maatschappelijke signalen, dat het wenselijk is ook die gevallen van spam (of bombing) strafbaar te stellen, waarin weliswaar niet de werking van een compleet netwerk of complete telecommunicatiedienst wordt verstoord maar wel de toegang van een individuele gebruiker tot zo'n netwerk of dienst wordt belemmerd. In zo'n geval wordt immers een elementair rechtsgoed in gevaar gebracht, namelijk de mogelijkheid van eenieder om ongehinderd gebruik te maken van een in de moderne samenleving belangrijk communicatiemedium. Daarom stel ik voor om na artikel 138a Sr betreffende computervredebreuk een nieuw artikel 138b op te nemen, strafbaar stellende het opzettelijk en wederrechtelijk, door tussenkomst van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, aan een ander gegevens toezenden die zijn bestemd om diens toegang tot dat netwerk of die dienst te belemmeren. Een verdergaande strafbaarstelling, die in het algemeen het ongevraagd toezenden van e-mail strafbaar stelt, acht ik niet opportuun. Hoe hinderlijk dit gedrag ook mag zijn, voor het strafrecht zie ik daarvoor thans geen rol weggelegd.

## 9. Handhaving

Over de uitvoerbaarheid en handhaafbaarheid van het hier voorgestelde merk ik het volgende op. In het wetsvoorstel wordt voorzien in een uitbreiding van het instrumentarium voor de opsporing en vervolging van criminaliteit waarbij de moderne informatie- en telecommunicatietechnologie een rol speelt (vgl. de voorgestelde ontoegankelijkmaking van gegevens, de medewerkingsverplichting t.a.v. de ontsleuteling van gegevens en de aangepaste pseudokoopbevoegdheid t.b.v. het onderzoek

op een openbaar computernetwerk). Daarnaast worden waarborgen gegeven voor een behoorlijk overheidsoptreden, met inachtneming van de (grond)rechten van de burgers (vgl. de beperking van de aansprakelijkheid van tussenpersonen en de nadere regulering van het onderzoek van e-mail). De voorgestelde wijzigingen brengen geen ingrijpende veranderingen mee voor de opsporing zoals die thans plaatsvindt. Het wetsvoorstel sluit aan op de huidige praktijk en op ontwikkelingen op het terrein van computercriminaliteit.
Ik verwacht dat de voorstellen zullen bijdragen aan een adequate aanpak – en waar nodig een verbetering daarvan – van criminaliteit in een geautomatiseerde omgeving, bijvoorbeeld op Internet. Over de effectiviteit van de voorstellen zijn geen ondubbelzinnige uitspraken te doen. Ten eerste is dat niet mogelijk omdat het totale aantal strafbare feiten of opsporingsonderzoeken waarvoor de onderhavige voorstellen mogelijk relevant zijn, niet of nauwelijks is vast te stellen of te schatten. Door de snelle verbreiding van het gebruik van moderne informatietechnologie (computers, GSM-telefoons, satellietcommunicatie, elektronische agenda's) speelt die technologie tegenwoordig immers ook bij traditionele criminaliteit vaak een rol. Verder geldt voor de uitings- en verspreidingsdelicten die worden gepleegd via een computernetwerk als Internet, dat de omvang en ernst van het probleem niet op zinvolle wijze per land is vast te stellen vanwege het grensoverschrijdende (zelfs wereldomspannende) karakter van deze delicten.
Naast een toereikend wettelijk instrumentarium vormen een adequate organisatie, goed opgeleide politie- en justitiefunctionarissen alsmede de beschikbaarheid van een kwalitatief hoogwaardige informatietechnologische uitrusting noodzakelijke voorwaarden voor een goede strafrechtelijke rechtshandhaving op de elektronische snelweg. Het aanpassen van uitrusting en opleidingsprogramma's aan de technologische ontwikkelingen maakt onderdeel uit van de bestedings- en opleidingsplannen. De opbouw van de organisatie van de handhaving – inclusief de personele en materiële middelen – is momenteel in volle gang. De regionale politiekorpsen beschikken inmiddels over zeven interregionale *bureaus digitale expertise,* die – in samenwerking met de CRI en de Afdeling Computeronderzoek van het Gerechtelijk Laboratorium – ondersteuning verlenen bij opsporingsonderzoeken waarbij informatietechnologie een rol speelt. Van belang is dat binnen de politie en justitie bestaande hiaten in de kennis van deze technologie door middel van bijscholing worden verholpen. Zoals de Stuurgroep Informatietechnologie en Criminaliteit in haar advies terecht opmerkt, geldt dit in het bijzonder ook voor de instanties waarbij de aansturing van en controle op de opsporing berust, namelijk de officier van justitie en de rechtercommissaris. Overigens leidt het wetsvoorstel zelf niet tot aanvullende eisen met betrekking tot de organisatie, uitrusting of opleiding van politie of justitie voor wat betreft de aanpak van computercriminaliteit. Dergelijke zaken zijn onder andere aan de orde in het actieprogramma «Op weg met digitaal rechercheren», dat uit de politie zelf is voortgekomen. Zoals bij een eerdere gelegenheid reeds toegezegd, zal ik de Kamer hierover nog een standpunt doen toekomen.
Bij het wetsvoorstel wordt een aantal nieuwe strafbaarstellingen gecreëerd (vernieling van stromende gegevens (artikelen 350a en 350b Sr), ernstige vormen van spam (artikel 138b Sr), uitbreiding van de strafbaarheid van vervalsing van chipcards en dergelijke (artikel 232 Sr) en de wederrechtelijke kennisneming door een telecommunicatieaanbieder van de inhoud van een e-mailbox van een abonnee (artikel 273d Sr)). Deze feiten zullen grotendeels door aangiften van slachtoffers aan het licht moeten komen. Vooralsnog verwacht ik geen grote aantallen en ga ik er vanuit dat deze feiten in de reguliere opsporings- en vervolgingspraktijk kunnen worden meegenomen.
De voorstellen brengen voor de burger slechts beperkte lasten mee. Zoals

aangegeven wordt de strafrechtelijke aansprakelijkheid van tussenpersonen die beroeps- of bedrijfsmatig informatie doorgeven, beperkt. In het algemeen is voldoende dat zij, zodra zij daartoe door justitie worden gemaand, adequate maatregelen nemen ter voorkoming van verdere verspreiding van dat materiaal. Stelselmatig, preventief onderzoek wordt van tussenpersonen niet geëist. Deze regeling sluit goed aan bij reeds bestaande vormen van zelfregulering van de Internet Service Providers op het terrein van onder andere kinderporno, waarbij zij waar mogelijk zelf actie ondernemen ter voorkoming van de verdere verspreiding van het strafbare materiaal. Bij adequate zelfregulering behoeft niet onmiddellijk naar het strafrecht te worden gegrepen en kan het strafrecht als sluitstuk fungeren.
Ook de voorgestelde verplichting om mee te werken aan het ontsleutelen van afgetapt gegevensverkeer brengt voor de burger slechts beperkte lasten mee. Zoals in paragraaf 4 aangegeven is de betrokkene slechts verplicht mee te werken voor zover hij daadwerkelijk beschikt over de benodigde kennis en voorzieningen. Voor zover hij niet over die kennis en voorzieningen beschikt is hij niet verplicht die alsnog te verwerven dan wel te installeren. Specifiek voor aanbieders van openbare telecommunicatienetwerken en -diensten geldt verder dat de voorgestelde medewerkingsverplichting geen extra eisen aan hun bedrijfsvoering stelt bovenop de eisen die daarvoor reeds gelden op grond van de nieuwe Telecommunicatiewet in het kader van de plicht van de aanbieders om hun netwerken en diensten aftapbaar te maken en houden. Voor de in een individueel geval verleende medewerking kan de betrokkene – telecommunicatieaanbieder of niet – een kostenvergoeding aanvragen op grond van de Wet tarieven in strafzaken. Om hoeveel gevallen per jaar het zal gaan, valt thans niet te zeggen. Uitgaande van jaarlijks 1000 bevelen tot medewerking en een kostenvergoeding van gemiddeld 50 gulden zullen de gerechtskosten voor de overheid met 50 000 gulden toenemen. Een vergelijkbare berekening kan gemaakt worden voor de verstrekking door telecomaanbieders van de inhoud van de e-mailbox van een abonnee op grond van het voorgestelde artikel 125i, derde lid, Sv. Beide kostenposten betekenen geen aanzienlijke uitbreiding van het budget voor gerechtskosten.

## ARTIKELSGEWIJS DEEL

### Artikel I

*A*

Dit onderdeel bevat de wijziging van de regeling van de uitgeversaansprakelijkheid zoals neergelegd in artikel 53 Sr. Aan dit onderwerp werd in het algemeen deel, paragraaf 2, reeds een uitvoerige beschouwing gewijd.
De bescherming tegen strafrechtelijke vervolging die artikel 53 Sr aan de tussenpersoon verleent, wordt uitgebreid tot de openbaarmaking of verspreiding van alle «uitingen in woord, beeld of geluid». Gezocht is naar een moderne, techniekonafhankelijke omschrijving van de uitingen die onderwerp zijn van de uitings- en verspreidingsdelicten. Onder «uitingen in woord» moeten zowel de in lettertekens geschreven woorden als het gesproken (of gezongen) woord worden verstaan. Daarbij is de gebruikte techniek irrelevant: woorden kunnen worden geproduceerd door traditionele middelen (bijv. pen en papier) en door meer moderne middelen zoals computers. Ook bijvoorbeeld «computerspeak» valt onder uitingen in woord. Onder «uitingen in beeld» vallen alle zichtbare (en soms ook tastbare) representaties van uitingen (anders dan in woorden), zoals tekeningen, foto, film, sculpturen enz. «Uitingen in geluid», tot slot,

omvatten alle hoorbare uitingen die niet reeds onder het gesproken woord vallen, zoals muziek. Overigens is het niet de bedoeling met de termen «woord, beeld en geluid» de betekenis van in bestaande delictsomschrijvingen voorkomende begrippen als «geschrift» of «mondelinge uitlating» te beperken.
De kern van de voorgestelde wijziging is de vervanging van de uitgever door de professionele tussenpersoon die informatie afkomstig van derden openbaar maakt of verspreidt. Ik ga op drie kenmerken van het begrip «tussenpersoon» nader in: 1. het beroepsmatig handelen, 2. het vermenigvuldigen ten behoeve van het publiek en 3. de intermediaire rol.
Ad 1. De «tussenpersoon» maakt zijn beroep of bedrijf van de openbaarmaking of verspreiding van informatie van derden aan derden. Het moet daarbij gaan om een hoofdwerkzaamheid van de (tussen)persoon, zij het wellicht een naast andere werkzaamheden. Speelt de verspreiding van informatie in het geheel van de werkzaamheden slechts een ondergeschikte rol, staat zij ten dienste van een andere werkzaamheid, dan is geen sprake van een professionele tussenpersoon. Een reclame- of *public relations* bureau, bijvoorbeeld, zal wellicht geschriften of afbeeldingen afkomstig van een cliënt onder het publiek verspreiden, maar dit is geen zelfstandige werkzaamheid van het bureau, maar staat ten dienste van de hoofdtaak: het bevorderen van de bekendheid en externe relaties van die cliënt. Een universiteit die in eigen beheer onderzoeksverslagen uitgeeft valt waarschijnlijk niet aan te merken als een tussenpersoon, een universitaire uitgeverij met een eigen organisatie en budget, een brede distributie en toegankelijk voor iedere onderzoeker binnen de universiteit, mogelijk wel.
Ad 2. De professionele tussenpersoon maakt informatie openbaar of verspreidt informatie. Dit wil zeggen dat hij de informatie voor het publiek beschikbaar maakt. Van openbaarmaking of verspreiding is geen sprake als de informatie slechts voor een of enkele bijzondere personen bestemd is; de informatie moet algemeen, voor een grotere groep mensen toegankelijk zijn. Een telecommunicatiebedrijf kan in het algemeen niet gezegd worden informatie openbaar te maken of te verspreiden. Voor wat betreft de normale telefonie verzorgt het slechts de communicatie tussen twee of meer (vgl. telefonisch vergaderen) bepaalde personen. Dit neemt niet weg dat hetzelfde bedrijf ook andere, zelfstandige diensten kan aanbieden die wel bestaan uit de verspreiding van informatie onder het publiek, en in zoverre wèl onder de bescherming van artikel 53 Sr kan vallen.
Ad 3. Het gaat bij de informatieverspreiding door de tussenpersoon om uitingen *afkomstig van derden.* De verspreiding van informatie waarvan de verspreider geheel of grotendeels zelf de bron is, valt niet onder de bescherming van artikel 53 Sr. De professionele tussenpersoon geeft informatie door aan het publiek. Daarvan is slechts sprake als de informatie in min of meer onbewerkte staat aan het publiek wordt aangeboden. Een journalist of een redacteur van een krant kan dan ook niet als een professionele tussenpersoon worden beschouwd: weliswaar is zijn informatie grotendeels afkomstig van derden, maar voordat die informatie publiek wordt gemaakt, wordt ze door de journalist of redacteur bewerkt, becommentarieerd, geselecteerd en gecombineerd. Hetzelfde zal gelden voor omroepinstellingen. Bij hun werk ligt de nadruk veel meer op het samenstellen van een gevarieerd programma dan op het doorgeven van informatie (films, shows enz.) van derden (het doorgeven speelt een ondergeschikte rol ten opzichte van het samenstellen en aanbieden van een volledig pakket, zie ad 1.). Zo bepaalt de Mediawet voor omroep*verenigingen* dat ze een totaalprogramma moeten verzorgen dat uit verschillende onderdelen bestaat (vgl. artikel 50 Mediawet).
Zie voor een bespreking van de drie voorwaarden die artikel 53 Sr stelt aan uitsluiting van vervolging, paragraaf 2.4. Het nieuwe tweede lid beperkt de strafrechtelijke aansprakelijkheid van tussenpersonen tot

uitingen waarop zijn opzet is gericht, dat wil zeggen dat hij eventueel – afhankelijk van de vraag of aan de voorwaarden van artikel 53 is voldaan – slechts kan worden vervolgd wegens zijn aandeel in de openbaarmaking of verspreiding van die uitingen waarvan hij de inhoud kent. Zie verder hierover paragraaf 2.5.

*B*

Dit betreft een correctie van de eerste Wet computercriminaliteit. Zij is mede ingegeven door een bespreking van prof. Kaspersen van deze wet (De Wet computercriminaliteit is er – nu de boeven nog, Computerrecht 1993/4, blz. 134 e.v.). De woorden «*al dan niet* op een overeengekomen wijze» in de definitie van het begrip «gegevens» zijn in feite zinledig. Gegevens krijgen hun betekenis door een onderliggende afspraak. Theoretisch is weliswaar denkbaar dat een computer wordt ontwikkeld die over een coderingssysteem beschikt dat op geen enkele wijze gegevens kan uitwisselen met andere computers – een computer met andere woorden die uitsluitend geschikt is voor het gebruik door één enkele persoon –, maar deze mogelijkheid mist maatschappelijke relevantie, zodat de woorden «al dan niet» in artikel 80quinquies kunnen worden gemist.

*C*

Dit onderdeel beoogt aan de definitie van een geautomatiseerd werk de overdrachtsfunctie toe te voegen. Deze functie is een wezenskenmerk van een geautomatiseerd werk, dat immers met name bestemd is om daarin opgeslagen of verwerkte gegevens aan de gebruiker terug te geven of aan een ander (computer-)systeem over te dragen.
De definitie spreekt van opslag, verwerking èn overdracht van gegevens. Het gaat hier om cumulatieve voorwaarden. Een inrichting die enkel bestemd is om gegevens over te dragen (een eenvoudig telefoontoestel, bepaalde zend- en ontvanginrichtingen) of op te slaan valt dus buiten de begripsomschrijving.

*D*

Artikel 138a Sr (computervredebreuk) wordt op enkele punten gewijzigd. In het eerste lid wordt tussen de woorden «opzettelijk wederrechtelijk» het woordje «en» opgenomen. Dit betekent dat niet meer bewezen behoeft te worden dat de verdachte wist dat zijn handelen wederrechtelijk was. Dit is een onnodig zware eis: bij iemand die een beveiliging doorbreekt of de toegang verwerft door een technische ingreep of iets dergelijks, mag wetenschap van het wederrechtelijke van zijn handelen worden verondersteld, behoudens natuurlijk een beroep op verontschuldigbare rechtsdwaling.
De woorden «voor de opslag of verwerking van gegevens» na «geautomatiseerd werk» vormen gelet op de definitie van artikel 80sexies een overbodige specificatie en kunnen dus worden geschrapt.
De wijziging van het tweede lid is in paragraaf 5.2 (over de gehanteerde terminologie) reeds toegelicht. De toevoeging van het «aftappen of opnemen» van gegevens die «worden verwerkt of overgedragen» door middel van het geautomatiseerd werk waarin wederrechtelijk is binnengedrongen, geeft aan dat op grond van het tweede lid naast het overnemen van in die computer opgeslagen gegevens ook strafbaar is het aftappen of opnemen van gegevens die ten tijde van de computervredebreuk binnenkomen (de «stromende» gegevens).
Het derde lid bevat twee gekwalificeerde vormen van computervredebreuk. Die onder a betreft het gebruik maken van de verwerkingscapaciteit van het geautomatiseerd werk waarin betrokkene is binnenge-

drongen. Voorgesteld wordt om het bestanddeel «met het oogmerk om zich wederrechtelijk te bevoordelen» aan te vullen met het oogmerk om een ander te bevoordelen.

*E*

De voorgestelde strafbaarstelling van bepaalde vormen van spam of bombing is in paragraaf 8 reeds toegelicht. Ik voeg daaraan nog het volgende toe. Het nieuwe artikel 138b Sr vereist niet dat door de betrokken gedraging de toegang tot het netwerk of de dienst daadwerkelijk wordt belemmerd, wel dat de dader iemand desbewust gegevens toezendt die, objectief gezien, bedoeld en geschikt zijn («bestemd zijn») om de toegang van die persoon tot het net te belemmeren. Zo'n geval zal zich bijvoorbeeld voordoen wanneer ongevraagd aan iemand een complete encyclopedie per e-mail wordt toegezonden, niet echter wanneer hem of haar ongevraagd een niet buitensporig grote hoeveelheid reclame wordt toegezonden; dit laatste is objectief gezien niet geschikt om de toegang tot Internet te belemmeren en brengt dus het beschermde rechtsgoed niet in gevaar. Niet vereist is overigens dat de betrokken handeling geschikt is om de toegang tot het net volledig te blokkeren, wel dat de reële mogelijkheid bestaat dat daardoor iemand gehinderd wordt in het gebruik van bijvoorbeeld Internet.
De maximumstraf voor het nieuwe strafbaar feit is gesteld op een jaar gevangenisstraf of geldboete van de vierde categorie. Dit is gelijk aan bijvoorbeeld de straf voorzien in artikel 139c Sr (het aftappen van telecom) en hoger dan die voor computervredebreuk (artikel 138a Sr).

*F tot en met I*

De artikelen 139a tot en met 139e Sr stellen het met een technisch hulpmiddel afluisteren, aftappen of opnemen van gesprekken en ander gegevensverkeer alsmede enkele daarmee samenhangende gedragingen strafbaar. In de onderdelen F tot en met I worden in deze artikelen enkele terminologische verbeteringen aangebracht, waarbij ze onder andere tekstueel beter op elkaar worden afgestemd. In de artikelen 139a, tweede lid, 139b, tweede lid, en 139c, eerste lid, wordt het woord «opzettelijk» naar voren gehaald. Het is redelijk de opzet-eis op de gehele delictsomschrijving te betrekken (vgl. ook reeds het bestaande artikel 139b, eerste lid, Sr). Tussen de woorden «opzettelijk» en «zonder daartoe gerechtigd te zijn» in de artikelen 139a en 139b wordt het woordje «en» geplaatst. Daarvoor geldt dezelfde reden als bij artikel 138a, eerste lid (zie onderdeel D). Verder wordt daar waar in de artikelen 139a tot en met 139e slechts sprake is van (het aftappen of opnemen van) gegevens die door middel van een geautomatiseerd werk worden *overgedragen,* ook genoemd het aftappen of opnemen van de geautomatiseerde gegevens*verwerking.* Zoals in paragraaf 13 aangegeven zijn «overdragen» en «verwerken» elkaar deels overlappende begrippen, maar omvat de laatste term ook gegevensverwerkingen door of binnen een computer waarbij geen sprake is van het transport van die gegevens van A naar B.

*J*

Met hetgeen in het voorgaande over de gehanteerde terminologie is gezegd spreken de wijzigingen in de artikelen 161sexies en 161septies vanzelf.

*K*

Artikel 232 Sr, bij de eerste Wet computercriminaliteit in het Wetboek opgenomen, stelt strafbaar de vervalsing van betaalpassen en waarde-

kaarten. Hiermee wordt gedoeld op allerlei magneet- en chipkaarten waarmee de rechthebbende langs geautomatiseerde weg financiële betalingen kan verrichten of, tegen betaling, bepaalde prestaties kan verkrijgen. Een voorbeeld van een betaalpas is de bankpas, een voorbeeld van een waardekaart een telefoonkaart (of bijvoorbeeld een kopieerkaart). Inmiddels gaan de ontwikkelingen rond met name chipcards in hoog tempo door en komen steeds meer kaarten op de markt met verschillende functies. Teneinde deze en toekomstige kaarten voldoende daarop toegesneden bescherming te geven wordt voorgesteld artikel 232 op enkele punten te verduidelijken en aan te vullen.
Waar artikel 232 nu alleen spreekt van kaarten «bedoeld voor het verrichten van betalingen», wordt voorgesteld dit uit te breiden tot kaarten «bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties». Hoewel de term «betalingen» ook in de ruimere betekenis van «prestaties» kan worden opgevat, wordt voorgesteld expliciet het verrichten of verkrijgen van andere prestaties dan financiële betalingen als mogelijke bestemming van dit soort kaarten op te nemen. De zinsnede «verrichten *of verkrijgen»* voorkomt onduidelijkheid over de vraag of nu sprake is van het doen van een betaling of het ontvangen van een prestatie. Een waardekaart bijvoorbeeld is vaak bij verkrijging reeds betaald en dient in dat geval strikt genomen enkel nog tot het verkrijgen van de tegenprestatie van de uitgever van de kaart (vgl. de telefoonkaart). De Beleidsadviesgroep digitaal rechercheren heeft er in zijn advies opgewezen dat deze kwestie in de praktijk tot problemen kan leiden bij het optreden tegen «gekloonde» telefoonkaarten.
Voorts wordt de werkingssfeer van artikel 232 Sr uitgebreid tot «enige andere voor het publiek beschikbare kaart» (bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties). Hierbij moet worden gedacht aan kaarten die noch als betaalpas noch als waardekaart kunnen worden aangemerkt, zoals passen waarop allerlei (bijvoorbeeld medische) informatie over de houder is vastgelegd. Ook in de toekomst te ontwikkelen kaarten kunnen de bescherming van artikel 232 Sr gaan genieten. Het moet dan wel gaan om kaarten die voor het publiek beschikbaar zijn, dat wil zeggen voor eenieder die dat wil beschikbaar, eventueel onder voorwaarden of tegen betaling (bijvoorbeeld van verzekeringspremies). Achtergrond hiervan is dat artikel 232 Sr strekt tot bescherming van het maatschappelijk vertrouwen in betaalpassen en dergelijke. Dit maatschappelijk vertrouwen is uiteraard niet in het geding bij kaarten die louter voor eigen gebruik of gebruik in besloten kring zijn bedoeld (bijvoorbeeld de toegangspassen van de werknemers van een bedrijf).
De wijziging van het tweede lid is van louter terminologische aard. Daarbij wordt uitgegaan van de bepaling zoals zij komt te luiden na het wet worden van het wetsvoorstel tot wijziging van het Wetboek van Strafrecht en andere wetten met het oog op de opneming in het Wetboek van Strafrecht van eenvormige strafbepalingen inzake het verstrekken van onware gegevens en het nalaten te voldoen aan wettelijke verplichtingen om tijdig gegevens te verstrekken (23 993, concentratie strafbaarstelling frauduleuze gedragingen).

*L*

De opneming in titel XVII (Schending van geheimen) van boek 2 van het Wetboek van Strafrecht van de nieuwe artikelen 273a tot en met 273e is in paragraaf 8 reeds toegelicht. Na de schending van het beroepsgeheim (artikel 272) en de schending van bedrijfsgeheimen (artikel 273) stellen deze artikelen strafbaar de schending van het communicatiegeheim (dat wil zeggen het brief-, telefoon-, telegraaf- en telecommunicatiegeheim) door personen die gelet op hun functie bij een post- of telecommunicatiebedrijf juist tot taak hebben een ongestoorde communicatie tussen personen mogelijk te maken zonder dat onbevoegden daarvan kennis

kunnen nemen of anderszins daarop inbreuk kunnen maken. Deze artikelen vervangen de ambtsdelicten van de artikelen 372 tot en met 375 Sr, die komen te vervallen (zie onderdeel R). Aan een dergelijke overhevelingsoperatie kleeft het bezwaar dat de rechtspraktijk zich op nieuwe bepalingen zal moeten instellen. Toch meen ik dat in dit geval de redenen van wetssystematiek die pleiten vóór overheveling, zwaarder wegen. Bovendien zijn de bepalingen inhoudelijk, behoudens het navolgende, niet gewijzigd, zodat ook de rechtspraak op de artikelen 372 tot en met 375 van toepassing kan blijven. Overigens betekent het feit dat de onderhavige delicten niet meer als ambtsdelict worden gekwalificeerd, dat zij niet meer vallen onder de generieke mogelijkheid van ontzetting uit bepaalde rechten bedoeld in artikel 29 Sr.
Afgezien van het «ambtelijk» element zijn de artikelen 273a, 273b, 273c en 273e gelijkluidend aan de artikelen 372, 373, 374 respectievelijk 375 Sr. Artikel 273d daarentegen, dat in de plaats komt van het huidige artikel 374bis Sr – welk artikel het aftapverbod voor personen werkzaam bij een telecommunicatieaanbieder bevat –, is om redenen als uiteengezet in paragraaf 6.2 uitgebreid met het door dergelijke personen wederrechtelijk *kennisnemen of overnemen* van niet voor hen bestemde gegevens die door tussenkomst van een telecommunicatienetwerk of -dienst zijn *opgeslagen.* Zoals aangegeven ziet deze uitbreiding op de situatie dat een telecommunicatieaanbieder zonder toestemming van de betrokkene kennisneemt van de op zijn computers opgeslagen persoonlijke gegevens van klanten (bijvoorbeeld e-mail in een e-mailbox). De in artikel 374bis nog voorkomende term «afluisteren» kon worden geschrapt omdat «kennisnemen» een neutrale term is die zowel op opgeslagen gegevens als op telecommunicatie betrekking kan hebben.

*M*

Dit betreft een aanvulling van artikel 285 Sr, strafbaarstellende bedreiging. Artikel 285 stelt onder andere strafbaar de bedreiging «met enig misdrijf waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht». Hiermee zijn bedoeld de misdrijven omschreven in titel VII van boek 2. Bij de eerste Wet computercriminaliteit zijn in die titel twee nieuwe gemeengevaarlijke misdrijven opgenomen, namelijk de (opzettelijke dan wel culpose) vernieling van een geautomatiseerd werk of een werk voor telecommunicatie (artikelen 161sexies en 161septies Sr). Daarbij is in die artikelen, naast het gemeen gevaar voor goederen of voor personen, expliciet het gemeen gevaar «voor de verlening van diensten» als grond voor strafbaarheid opgenomen. Toen is echter nagelaten deze grond ook in artikel 285 Sr op te nemen. De Hoge Raad leidt hier in een recent arrest (HR 2 december 1997, NJ 1998, 306) uit af dat, mede gelet op de geboden restrictieve uitleg van strafbepalingen, het dreigen met de vernieling van een computer waardoor gemeen gevaar voor de verlening van diensten ontstaat, niet strafbaar is op grond van artikel 285 (dus ook niet onder gemeen gevaar voor goederen kan worden begrepen). Deze uitspraak wijst naar mijn mening op een lacune in artikel 285 Sr, die – gelet op de huidige maatschappelijke betekenis van dienstverlening zoals die ook bij de Wet computercriminaliteit erkenning heeft gekregen – opvulling behoeft. Dit onderdeel strekt hiertoe.

*N en O*

De uitbreiding van de artikelen 350a en 350b Sr, strafbaarstellende het (opzettelijk dan wel culpoos) veranderen, wissen, onbruikbaar of ontoegankelijk maken van computergegevens, tot gegevens die worden verwerkt of overgedragen «door middel van telecommunicatie» is in paragraaf 8 reeds toegelicht. Voorgesteld wordt verder om in beide artikelen de zinsnede betreffende het strafbare «toevoegen van gegevens»

te schrappen, omdat niet geheel duidelijk is welke «toevoegingen», mede gelet op de door deze artikelen beschermde belangen (de integriteit en beschikbaarheid van gegevens), wederrechtelijk en daarmee strafbaar moeten worden geacht (als niet tevens sprake is van het veranderen, wissen enz. van gegevens).
De in artikel 350a, derde lid, en artikel 350b, tweede lid, vervatte strafbare feiten van het ter beschikking stellen of verspreiden van schadelijke gegevens zoals computervirussen worden zowel aangescherpt als verruimd. Aangescherpt omdat de zinsnede «bedoeld zijn om schade aan te richten» is gewijzigd in: bestemd zijn om schade aan te richten. Het woord «bestemd» is nauwkeuriger en toont zowel de bedoeling van de dader als de geschiktheid van het middel. Van een verruiming is sprake waar de zinsnede «door zichzelf te vermenigvuldigen» komt te vervallen. Behalve door gegevens die schadelijk zijn door hun vermenigvuldiging in een geautomatiseerd systeem kan immers ook schade aan een systeem worden toegebracht door programma's die een of meer systeemfuncties uitvoeren, waardoor bijvoorbeeld de gegevens op het externe geheugen verloren gaan of het systeem vastloopt. Ook het ter beschikking stellen of verspreiden van zogenaamd logische bommen en trojaanse paarden (bijvoorbeeld het programma «Back Orifice») valt met deze wijziging onder het bereik van artikel 350a, derde lid, en 350b, tweede lid.

*P*

Zoals eerder aangegeven kan ten aanzien van het begrip geautomatiseerd werk de specificatie «voor de opslag of verwerking van gegevens» als overbodig worden geschrapt.

*Q*

Artikel 371 Sr stelt strafbaar de ambtenaar die zijn bevoedheid misbruikt om van ambtenaren en andere personen werkzaam in de post- en de telecommunicatiesector informatie over het post- en telecommunicatie-verkeer te verkrijgen. Nu, zoals in paragraaf 8 aangegeven, deze sectoren grotendeels zijn geprivatiseerd en daarin dus geen ambtenaren meer werkzaam zijn, dient artikel 371 dienovereenkomstig te worden gewijzigd.

*R en S*

De overheveling van de bepalingen betreffende schending van het brief-, telefoon- en telegraafgeheim (artikelen 372 tot en met 375 Sr) naar titel XVII is hiervoor reeds toegelicht (zie onder L). Onderdeel S betreft een technische wijziging als gevolg van deze overhevelingsoperatie.

*T en U*

Artikel 418 Sr is het spiegelbeeld van artikel 53 Sr: als aan een van de voorwaarden voor uitsluiting van vervolging niet is voldaan, is de tussenpersoon *als zodanig* strafbaar wegens de openbaarmaking of verspreiding van strafbare informatie. Verwezen zij verder naar de toelichting op artikel 53, in het bijzonder naar hetgeen in paragraaf 2.4 is opgemerkt over de inhoud en de reikwijdte van de voorwaarden van artikel 53, eerste lid. Zoals aangegeven in paragraaf 2.5 wordt voorgesteld om de strafbaarheid van de tussenpersoon voortaan te beperken tot opzettelijk handelen in de zin dat zijn opzet (mede) gericht dient te zijn op het strafbare karakter van de betrokken uiting.
De wijziging van artikel 420 Sr (onderdeel U) betreft een technische wijziging als gevolg van de wijziging van artikel 418.

*V*

Artikel 421 Sr bevat een generieke strafverhoging in geval van recidive bij bepaalde misdrijven uit winstbejag. De overheveling van de strafbaarstelling van artikel 373, tweede lid, – betreffende de persoon, werkzaam bij een openbare instelling van vervoer, die zich een poststuk of daarin gesloten voorwerp met geldswaarde toe-eigent – naar artikel 273b, tweede lid, noopt tot deze technische aanpassing.

**Artikel II**

Bij de voorgestelde wijzigingen van het Wetboek van Strafvordering is uitgegaan van de tekst van het wetboek zoals die luidt na inwerkingtreding van de Wet herziening gerechtelijk vooronderzoek en de Wet bijzondere opsporingsbevoegdheden (wetten van 27 mei 1999, Stb. 243 resp. 245).

*A*

De beperking van de bevoegdheid van artikel 125i, eerste lid, Sv tot gegevens «die ten tijde van het bevel zijn opgeslagen in een geautomatiseerd werk» is in paragraaf 5.2 reeds toegelicht. De overige wijzigingen in de formulering van de eerste twee leden van artikel 125i betreffen correcties van taalkundige aard, voorgesteld naar aanleiding van opmerkingen gemaakt in de Eerste Kamer bij gelegenheid van de mondelinge behandeling van het wetsvoorstel computercriminaliteit (Handelingen I 1992/93, p. 11-452 e.v.). Inhoudelijke wijzigingen worden niet beoogd.
Het voorgestelde derde lid betreft de nadere regeling van het onderzoek van gegevens (bijvoorbeeld e-mail) opgeslagen in het geautomatiseerde werk van een telecommunicatieaanbieder. Zie paragraaf 6.2.

*B*

Artikel 125j Sv gaat over het onderzoek van gegevens in geautomatiseerde werken in geval van een huiszoeking (in de terminologie van de Wet herziening gerechtelijk vooronderzoek een «doorzoeking») en met name over de mogelijkheid van een zogenaamde netwerkzoeking vanaf de plaats van de huiszoeking in computers elders. Doel van deze bevoegdheid tot het doen van onderzoek in computers is het vergaren van voor de waarheidsvinding relevante gegevens die op de plaats van de doorzoeking (of op daarmee via een computernetwerk verbonden plaatsen) *reeds aanwezig* zijn en níet het onderscheppen van gegevens die op het moment van de doorzoeking door de ter plaatse aanwezige computers worden verwerkt dan wel via een netwerk worden ontvangen of overgedragen (de «stromende» gegevens). Deze beperking volgt uit het feit dat de bevoegdheid tot het doen van onderzoek in computers wordt afgeleid uit de bevoegdheid tot inbeslagneming van daarvoor vatbare voorwerpen zoals een computer; de inbeslagnemingsbevoegdheid mag uit de aard der zaak slechts worden uitgeoefend indien redelijkerwijs kan worden vermoed dat op de te doorzoeken plaats daarvoor vatbare voorwerpen *aanwezig zijn.* Zou de doorzoekingsbevoegdheid worden gebruikt om gedurende enige tijd (tijdens de doorzoeking) binnenkomende en uitgaande gegevens te onderscheppen, dan zou feitelijk sprake zijn van het opnemen of aftappen van telecommunicatie. Daarvoor is echter artikel 125g Sv bedoeld. Teneinde dit beter in de tekst van artikel 125j tot uitdrukking te brengen worden de woorden (onderzoek naar) «in dat werk opgeslagen» (gegevens) ingevoegd. Hiermee is overigens niet gezegd dat wanneer de politie bij een onderzoek naar in een computer aanwezige gegevens stuit op gegevens die daar op dat moment binnen-

komen, deze niet met het oog op de bewijsgaring zou mogen vastleggen. Dan is sprake van een zogenaamde toevallige vondst en die mag volgens vaste rechtspraak voor het bewijs of verdere opsporingshandelingen worden gebruikt.
De herformulering van het tweede lid betreft een taalkundige verbetering.

*C*

Op grond van artikel 125k kan iemand worden bevolen toegang te verschaffen tot een geautomatiseerd werk en de daarin aanwezige gegevens door zijn kennis omtrent de beveiliging, of, ingeval de gegevens in het geautomatiseerd werk zijn versleuteld, de kennis omtrent de wijze van versleuteling ter beschikking te stellen. Artikel 125k geldt bij een huiszoeking (doorzoeking volgens de Wet herziening gerechtelijk vooronderzoek) of bij toepassing van artikel 125j. In de praktijk komt het regelmatig voor dat bij een huiszoeking enkel de gegevens worden gekopieerd, waarna een nader onderzoek van die gegevens vervolgens op het politiebureau geschiedt. Ook in deze gevallen dient artikel 125k toepasselijk te zijn. Teneinde hierover alle misverstand te vermijden is dit artikel daarom gewijzigd in die zin dat het bevel als bedoeld kan worden gegeven «bij of terstond na een doorzoeking of de toepassing van artikel 125j». De woorden «terstond na» komen ook voor in de definitie van ontdekking op heterdaad (artikel 128, eerste lid, Sv). Wat nog «terstond» is, hangt af van de omstandigheden van het geval, de ernst van het feit en de complexiteit van het onderzoek. Waar het om gaat is dat de opsporingsambtenaren onverwijld overgaan tot het onderzoek van het bij een doorzoeking vergaarde materiaal en daarmee niet nodeloos wachten.

*D*

Het huidige derde lid van artikel 125m Sv, betreffende de opgave aan de beheerder van een geautomatiseerd werk van de ten behoeve van de strafvordering vastgelegde gegevens, wordt, met enkele verruimingen, overgeheveld naar het nieuwe artikel 125p.

*E*

De zevende afdeling van titel IV van boek 1 van het Wetboek van Strafvordering, getiteld «Onderzoek van gegevens in geautomatiseerde werken», bevat thans nog een betrekkelijk summiere regeling. Afgezien van de bevoegdheid van de rechter-commissaris op grond van artikel 125i is de regeling vooral gericht op de huiszoeking (c.q. doorzoeking) en wat daarbij mogelijk is ten aanzien van geautomatiseerde werken. Over wat er moet c.q. mag gebeuren met gegevens die in geautomatiseerde werken worden aangetroffen, is weinig geregeld. Met name echter de kwesties van de bewaring en vernietiging van gegevens vragen naar de huidige inzichten (zoals onder andere blijkend uit de Wet bijzondere opsporingsbevoegdheden) om een tamelijk precieze regeling.
De bepalingen zoals thans neergelegd in de artikelen 125m, derde lid, en 125n worden vervangen door vier nieuwe artikelen. Deze zien alle op gegevens die worden aangetroffen dan wel vastgelegd «bij een onderzoek in een geautomatiseerd werk». Hieronder vallen niet alleen de toepassing van artikel 125i en het onderzoek bij gelegenheid van een doorzoeking, maar ieder onderzoek in een computer waartoe opsporingsambtenaren in het kader van een opsporingsonderzoek – met toepassing van een dwangmiddel dan wel met toestemming van de betrokkene – toegang hebben gekregen. Hierbij kan men bijvoorbeeld ook denken aan het onderzoek van een lap-top-computer die bij de aanhouding van de verdachte bij deze in beslag is genomen. Alleen het onderzoek van

telecommunicatie (artikelen 125f en 125g Sv) is apart geregeld en wordt niet geregeerd door de artikelen 125n en volgende.

### Artikel 125n Sv

Artikel 125n gaat, net als het voorgestelde artikel 125i, derde lid, over gegevens (m.n. e-mail) die zich bevinden in het geautomatiseerd werk van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst. Tezamen en in identieke bewoordingen geven beide bepalingen aan van welke van die gegevens politie en justitie mogen kennisnemen ten behoeve van de waarheidsvinding. Daarbij moet het gaan om gegevens die in een bepaalde relatie tot de verdachte dan wel het strafbare feit staan, welke relatie bovendien «klaarblijkelijk» aanwezig moet zijn. Zie hierover paragraaf 6.2. De artikelen 125i, derde lid, en 125n verschillen van elkaar voor zover betreft het toepassingsbereik. Waar de eerste bepaling specifiek ziet op de toepassing van de bevoegdheid van artikel 125i, eerste lid, ten aanzien van telecommunicatieaanbieders, ziet artikel 125n in het algemeen op «bij een onderzoek in het geautomatiseerd werk van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst (...) aangetroffen» gegevens (die niet voor deze aanbieder bestemd of van hem afkomstig zijn). Daarbij moet met name worden gedacht aan het onderzoek bij gelegenheid van een huiszoeking bij een telecommunicatieaanbieder.

### Artikel 125o

In het nieuwe artikel 125o Sv is de voorlopige maatregel van ontoegankelijkmaking van gegevens neergelegd. Deze is in het algemeen deel van de toelichting (paragraaf 3) reeds toegelicht. Daaraan zij hier alleen toegevoegd dat de woorden «dan wel» in het eerste en derde lid aangeven dat lopende een gerechtelijk vooronderzoek de rechter-commissaris exclusief bevoegd is en de officier van justitie dus geen beslissingen over ontoegankelijkmaking mag nemen.
In dit wetsvoorstel worden, ten behoeve van de ontoegankelijkmaking en de vernietiging van gegevens, géén nieuwe zoekbevoegdheden voorgesteld. Beide maatregelen hebben slechts betrekking op gegevens die bij een onderzoek in een geautomatiseerd werk «worden aangetroffen». Dergelijk onderzoek moet op andere gronden berusten, zoals de mogelijkheid voor de RC om de «uitlevering» van computergegevens te bevelen (artikel 125i Sv) of de doorzoekings- of inbeslagnemingsbevoegdheden. Ook is het mogelijk dat bij een zogenaamde netwerkzoeking – onderzoek vanaf de plaats van een huiszoeking in een elders aanwezig geautomatiseerd werk (artikel 125j Sv) – in een computer elders strafbare gegevens worden aangetroffen. De hier voorgestelde bevoegdheid maakt het dan mogelijk die gegevens ontoegankelijk te maken. Ook is het mogelijk dat via Internet strafbare informatie wordt gevonden. Wanneer redelijkerwijs kan worden vermoed dat het gaat om gegevens die onder Nederlandse rechtsmacht vallen, kan ook dàn deze maatregel worden getroffen (zie ook paragraaf 7.1). In andere gevallen is de Nederlandse justitie afhankelijk van het ingrijpen van de ter plaatse bevoegde rechterlijke autoriteiten.

### Artikel 125p Sv

Op grond van de Aanbeveling nr. R (95) 13 van de Raad van Europa betreffende strafprocesrecht en informatietechnologie behoren belanghebbenden in beginsel te worden geïnformeerd over vastlegging of ontoegankelijkmaking van computergegevens. Belanghebbend is allereerst de beheerder van het computersysteem, als degene die uit hoofde van zijn functie primair verantwoordelijk is voor het behoud en het

gebruik van de gegevens die zijn opgeslagen in de aan zijn zorg toevertrouwde computers. Daarnaast kunnen anderen belanghebbend zijn (zie 65 e.v. van het Explanatory memorandum). De bedoelde informatieplicht (tegenwoordig ook wel notificatieplicht genoemd) moet worden gezien tegen het licht van artikel 13 EVRM, dat voorschrijft dat eenieder wiens rechten en vrijheden zijn geschonden, recht heeft op een «effective remedy» voor een nationale instantie. De notificatieplicht waarborgt dat de betrokkene van een dergelijke (mogelijke) schending op de hoogte komt.
Het huidige artikel 125m, derde lid, Sv is beperkt doordat het alleen een opgaveplicht schept ten aanzien van de beheerder. Voorgesteld wordt nu om in een nieuw artikel 125p een brede mededelingsplicht op te nemen, die zowel geldt bij de enkele vastlegging – ten behoeve van het onderzoek naar een strafbaar feit – van gegevens die bij een onderzoek in een geautomatiseerd werk zijn verkregen, als bij de ontoegankelijkmaking van dergelijke computergegevens, en die niet alleen verplicht tot mededeling aan de beheerder van de computer maar ook tot mededeling aan bepaalde andere betrokken personen. Daarbij is zoveel mogelijk aangesloten bij de notificatieplicht die in de Wet bijzondere opsporingsbevoegdheden is opgenomen ten aanzien van de uitoefening van bijzondere opsporingsbevoegdheden (zie artikel 126bb Sv). Wat betreft de vraag welke andere categorieën personen dan de beheerder – actief – op de hoogte moeten worden gesteld van de vastlegging (of ontoegankelijkmaking) van computergegevens laat de Aanbeveling van de Raad van Europa staten een grote vrijheid. Buitensporige inspanningen worden niet van de autoriteiten geëist. De notificatieverplichting moet wel werkbaar blijven. Gelet hierop en in lijn met de Wet bijzondere opsporingsbevoegdheden wordt in artikel 125p het begrip «betrokkene» gebruikt en wordt in het derde lid limitatief aangegeven wie als zodanig moeten worden aangemerkt. Behalve de beheerder van het geautomatiseerd werk (sub b) is dit de rechthebbende van de plaats waar de doorzoeking heeft plaatsgevonden waarbij de gegevens zijn vastgelegd (sub c) en de verdachte (sub a). Wat deze laatste betreft behoeft geen mededeling plaats te vinden indien hij door opneming van de gegevens in de processtukken daarvan toch reeds op de hoogte komt (lid 4). Naast deze categorieën zijn meer personen denkbaar die er mogelijk belang bij hebben te weten dat bepaalde gegevens voor het onderzoek zijn vastgelegd. Daarbij moet men denken aan personen van wie de naam of andere gegevens in een aangetroffen gegevensbestand opduiken en die mede daardoor in relatie worden gebracht met de verdachte. Er is van afgezien deze moeilijk te bepalen groep als betrokkene in de zin van artikel 125p aan te merken. Als het gaat om getuigen zullen zij, zodra ze door de politie worden gehoord, van het onderzoek in kennis worden gesteld. Als het gaat om personen die zelf als verdachte worden aangemerkt (eventueel in een ander onderzoek), geldt ten aanzien van hen op de voet van het derde lid, onderdeel a, een notificatieplicht.
De mededeling behoeft geen uitputtende opgave van alle vastgelegde dan wel ontoegankelijkgemaakte gegevens te bevatten. Volstaan kan worden met een aanduiding van de aard van de betrokken gegevens, dat wil zeggen met een globale aanduiding, die de betrokken persoon in staat stelt te beoordelen of zijn rechten (naar zijn oordeel) zijn geschonden. Dit is in overeenstemming met eerdergenoemde Aanbeveling van de Raad van Europa, die spreekt van het informeren over «the *kind* of data that has been seized.»
Niet uitdrukkelijk is bepaald wie de mededeling doet. Dit zal hetzij de politie zijn hetzij, indien de vastlegging van de betrokken gegevens op last van de officier van justitie dan wel de rechter-commissaris is geschied, deze officier of RC. Mededeling geschiedt schriftelijk en zo spoedig mogelijk. Deze laatste clausule laat geen uitstel toe met het oog op het opsporingsbelang. Uitstel is slechts mogelijk onder de (hierna te

bespreken) voorwaarde van het tweede lid. Mededeling kan echter geheel achterwege blijven indien het doen van mededeling redelijkerwijs niet mogelijk is (eerste lid, laatste volzin), bijvoorbeeld omdat het achterhalen van de betrokkene onevenredig veel inspanning zou vergen.
Artikel 125p Sv is een uitdrukking van de gedachte dat in beginsel geen geheim opsporingsonderzoek behoort plaats te vinden. Geheimhouding is slechts gerechtvaardigd wanneer de goede uitoefening van een opsporingsbevoegdheid in gevaar zou komen door het bekend worden daarvan bij de te onderzoeken subjecten, zoals bijvoorbeeld bij een telefoontap. De uitoefening van deze bevoegdheid zou van iedere betekenis zijn ontbloot wanneer degeen die wordt afgeluisterd, daarvan zou weten. In zo'n geval kan de effectuering van het grondrecht als verwoord in artikel 13 EVRM tijdelijk worden opgeschort, omdat zulks noodzakelijk is in verband met de goede uitvoering het opsporingsonderzoek. Het voorgestelde tweede lid van artikel 125p voorziet in een dergelijke opschorting «indien en zolang het belang van het onderzoek zich tegen mededeling aan deze betrokkene verzet.» Dit criterium is ontleend aan artikel 126bb, eerste lid, zoals voorzien bij de Wet bijzondere opsporingsbevoegdheden. Vanwege het uitzonderingskarakter van de uitstelmogelijkheid is het oordeel hierover voorbehouden aan de officier van justitie dan wel, tijdens een gerechtelijk vooronderzoek, de rechter-commissaris.
Tot slot wijs ik erop dat de vastlegging van gegevens voor opsporingsdoeleinden zoals bedoeld in artikel 125p Sv niet geregeerd wordt door het regime van het bij de Tweede Kamer aanhangige voorstel voor een Wet bescherming persoonsgegevens (kamerstukken II 1997/98, 25 892, nrs 1–2). Deze wet strekt namelijk ter uitvoering van EG-richtlijn nr. 95/46/EG, welke richtlijn geen betrekking heeft op hetgeen binnen de zogenaamde derde pijler van de Europese Unie valt, waaronder onder andere de opsporing en vervolging van strafbare feiten. Dit betekent in het bijzonder dat de algemene notificatieplicht van artikel 34 Wet bescherming persoonsgegevens niet van toepassing is op de vastlegging van (persoons)gegevens die bij een opsporingsonderzoek zijn aangetroffen in een geautomatiseerd werk. Dit neemt niet weg de grondgedachte achter deze bepaling dezelfde is als die achter artikel 125p Sv.

### Artikel 125q

Artikel 125q geeft een uitgewerkte regeling van de bewaring en vernietiging van de bij een onderzoek in een geautomatiseerd werk vastgelegde gegevens. Zij is gelijkluidend aan de regeling zoals voorzien in de artikelen 126cc en 126dd ten aanzien van gegevens verkregen met behulp van bijzondere opsporingsbevoegdheden. Zolang de zaak niet is geëindigd, worden de gegevens, voor zover niet in de processtukken opgenomen, bewaard en ter beschikking van het onderzoek gehouden (artikel 125q, eerste lid). Dit geeft onder andere aan de verdediging de mogelijkheid om bepaalde gegevens alsnog bij de processtukken te doen voegen.
«Bewaren» betekent niet dat de gegevens mogen worden opgeslagen in een gewoon politieregister als bedoeld in de Wet politieregisters en zonder beperking mogen worden gebruikt voor andere strafrechtelijke onderzoeken. Het voorgestelde derde lid geeft limitatief aan voor welke andere doeleinden de gegevens mogen worden gebruikt. Dit laat onverlet dat de gegevens worden opgeslagen in een tijdelijk register in de zin van artikel 13 van de Wet politieregisters, zoals dat zal komen te luiden na inwerkingtreden van de Wet van 27 mei 1999 (Stb. 244). Twee maanden nadat de zaak is geëindigd en de laatste mededeling aan een betrokkene bedoeld in artikel 125p is gedaan, worden de gegevens vernietigd, hetzij door de opsporingsambtenaar die ze heeft vastgelegd zèlf, hetzij, indien vastlegging op last van de officier van justitie of de RC is geschied, door deze (lid 2).

Het derde lid maakt een uitzondering mogelijk op de regel dat de bij een onderzoek in een geautomatiseerd werk vergaarde gegevens uitsluitend gebruikt mogen voor het onderzoek naar het strafbaar feit waarop het betrokken computeronderzoek was gericht. Limitatief is aangegeven voor welke andere doelen die gegevens mogen worden gebruikt, namelijk a. voor een *ander* strafrechtelijk onderzoek of b. voor opslag in een register zware criminaliteit, indien het gegevens betreft omtrent een persoon als bedoeld in artikel 13a, eerste lid, onderdeel a tot en met c, Wet politieregisters. Bij deze laatste categorie gaat het om de groep van personen die nog niet als verdachte kunnen worden aangemerkt, maar omtrent wie wel gegevens (mogen) worden opgenomen in een register zware criminaliteit in de zin van de Wet politieregisters. De aldus vormgegeven regeling betreffende de verstrekking voor andere doeleinden dan het oorspronkelijke strafrechtelijk onderzoek in het kader waarvan de gegevens zijn vergaard, loopt in grote lijnen parallel – behoudens enkele aanscherpingen – aan het verstrekkingsregime voor tijdelijke registers zoals voorzien bij de Wet politieregisters. Omdat de bepaling van het Wetboek van Strafvordering een speciale regeling is ten opzichte van de regeling van de Wet politieregisters, derogeert zij aan het ruimere regime van de Wet politieregisters. De iets striktere regeling wordt gerechtvaardigd door de indringendheid van de opsporingsmethode met behulp waarvan de gegevens zijn vergaard.
Tot slot wijs ik erop dat het de officier van justitie is die bepaalt of de betrokken gegevens voor een ander doel als bedoeld in het derde lid kunnen worden gebruikt. In geval van toepassing van het derde lid geldt vanzelfsprekend uitstel van de vernietigingsplicht (vierde lid). Voor de details en achtergronden van deze regeling verwijs ik naar de toelichting op het wetsvoorstel dat heeft geleid tot de Wet bijzondere opsporingsbevoegdheden.

*F*

Dit onderdeel, tezamen met onderdeel H, bevat de in paragraaf 7.2 van het algemeen deel toegelichte aanpassing van de pseudokoopbepalingen zoals neergelegd in de Wet bijzondere opsporingsbevoegdheden met het oog op het onderzoek op openbare computernetwerken.

*G*

De onderdelen G en I bevatten de verplichting voor degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van gegevensverkeer dat onderwerp is van een tap, om mee te werken aan de ontsleuteling daarvan. Zie paragraaf 4. Uitgegaan is van de tapbepalingen zoals die luiden na invoering van de Wet bijzondere opsporingsbevoegdheden. Het bevel tot medewerking dient «bij of terstond na» het aftappen van het betrokken gegevensverkeer te worden gegeven. Zie voor de betekenis van deze woorden de wijziging van artikel 125k, eerste lid, en de toelichting daarop (onderdeel C).

*H*

Zie onderdeel F.

*I*

Zie onderdeel G.

*J*

Het huidige artikel 353 Sv verzekert dat bij de einduitspraak steeds een

beslissing wordt genomen over inbeslaggenomen voorwerpen. Het hier voorgestelde artikel 354 doet hetzelfde ten aanzien van ontoegankelijk gemaakte computergegevens. Als de rechter niet besluit tot vernietiging moet hij de gegevens weer ter beschikking van de beheerder doen stellen.

*K*

Artikel 552a Sv bevat de mogelijkheid voor belanghebbenden om bij de raadkamer van het betrokken gerecht te klagen over kortweg de inbeslagneming van voorwerpen en het gebruik daarvan alsmede over de kennisneming en het gebruik van bepaalde bij een opsporingsonderzoek vergaarde gegevens. Deze mogelijkheid moet worden gezien tegen het licht van artikel 13 EVRM. Wat gegevens uit een computer betreft beperkt de beklagmogelijkheid zich thans tot gegevens vastgelegd tijdens een huiszoeking (evt. met toepassing van artikel 125j Sv) en gegevens verkregen met toepassing van artikel 125i Sv. Nu, zoals hiervoor uiteengezet (zie onderdeel E), de regeling van het onderzoek van gegevens in geautomatiseerde werken zoals neergelegd in de artikelen 125i tot en met 125q is verbreed tot ieder «onderzoek in een geautomatiseerd werk», past het om ook de beklagmogelijkheid dienovereenkomstig te verbreden. Artikel 552a is daartoe opnieuw geformuleerd (onderdeel 1).
Zoals in paragraaf 3.2 reeds aangegeven, wordt verder voorgesteld om de beklagmogelijkheid uit te breiden tot de ontoegankelijkmaking van strafbare gegevens op grond van artikel 125o Sv. Deze beklagmogelijkheid strekt primair tot bescherming van de rechten van degenen die, voordat de maatregel werd toegepast, toegang hadden tot de betrokken gegevensbestanden. De voorgestelde regeling biedt – naast het beklag over de ontoegankelijkmaking zelf – ook de mogelijkheid te klagen over het uitblijven van een last tot opheffing van de ontoegankelijkmaking en over de (voorgenomen) opheffing van de ontoegankelijkmaking. Dit laatste is met name van belang voor het slachtoffer dat er een direct belang bij heeft dat hij niet weer voorwerp wordt van een strafbaar feit.
Het is van belang dat, indien eenmaal een klaagschrift is ingediend, andere belanghebbenden dan de klager zoveel mogelijk bij de behandeling van dat klaagschrift worden betrokken. Artikel 552a, vierde lid, tweede volzin, bevat daarom een aanwijzing aan de voorzitter van het gerecht om andere belanghebbenden van het klaagschrift in kennis te doen stellen. Dit voorschrift behoort ook te gelden bij klaagschriften die betrekking hebben op vastgelegde of ontoegankelijk gemaakte computergegevens. Dit wordt duidelijk gemaakt door de invoeging van de woorden «of dezelfde gegevens».

*L*

In het voorgestelde systeem van ontoegankelijkmaking en vernietiging van computergegevens is de definitieve beslissing voorbehouden aan de rechter. Dit betekent dat, net als bij de onttrekking aan het verkeer van voorwerpen, voorzien moet zijn in de mogelijkheid van vernietiging bij afzonderlijke rechterlijke beschikking voor het geval het niet tot een strafzaak komt. Hiertoe wordt artikel 552fa Sv voorgesteld, dat voor wat betreft de procedure aanknoopt bij artikel 552f Sv (over de onttrekking aan het verkeer).

**Artikel III**

De wijziging van de Telecommunicatiewet is een sequeel van het nieuwe derde lid van artikel 125i Sv, in welk lid bepaalde beperkingen worden gesteld aan de toepassing van artikel 125i (de vordering «uitlevering» van computergegevens) ten aanzien van aanbieders van openbare telecommunicatiediensten of openbare telecommunicatienetwerken.

Uitgangspunt van hoofdstuk 13 van de Telecommunicatiewet is dat indien strafvorderlijke bevoegdheden specifieke verplichtingen meebrengen voor telecomaanbieders, deze verplichtingen in die wet uitdrukkelijk worden omschreven. In zoverre is de Telecommunicatiewet volgend ten opzichte van het Wetboek van Strafvordering. Nu derhalve de algemene bevoegdheid van artikel 125i, eerste lid, Sv in het nieuwe derde lid van dat artikel nader wordt geregeld voor zover zij betrekking heeft op telecomaanbieders, dient een daarmee corresponderende bepaling te worden opgenomen in de Telecommunicatiewet. Daartoe wordt artikel 13.2a voorgesteld.
Een bevel als bedoeld in artikel 125i Sv kan slechts betrekking hebben op gegevens die de persoon tot wie het bevel is gericht, *voorhanden* heeft. Dit betekent voor telecomaanbieders dat zij slechts gehouden zijn om die gegevens uit te leveren die op het moment van het bevel in hun systemen zijn opgeslagen. Het gaat hier om een momentopname; gegevens (bijvoorbeeld e-mails) die zich in het verleden mogelijk op hun computers bevonden, maar inmiddels door een abonnee daarvan zijn gewist, kunnen niet op grond van artikel 125i, derde lid, worden opgevraagd. Ook gegevens die zich op een computer elders bevinden waarmee de computer van de telecomaanbieder is verbonden, kunnen niet bij deze telecomaanbieder worden opgevraagd. Verdergaande verplichtingen dan de plicht om de gegevens die voorhanden zijn te verstrekken, liggen niet in de artikelen 125i Sv en 13.2a Telecommunicatiewet besloten. Telecomaanbieders zijn dus niet gehouden om hun systemen aan te passen of aparte voorzieningen te treffen teneinde aan een bevel op grond van artikel 125i te kunnen voldoen of op ruimere schaal aan zo'n bevel te kunnen voldoen. In dit verband wijs ik nog op artikel 13.1 Telecommunicatiewet inhoudende de eis dat netwerken en diensten «aftapbaar» zijn. De hier uiteengezette beperkte strekking van de artikelen 125i Sv en 13.2a Telecommunicatiewet brengt mee dat die aftapbaarheid van artikel 13.1 geen betrekking heeft op de uitvoering van een bevel op grond van artikel 125i. In zoverre brengt het voorgestelde artikel 13.2a dus geen extra lasten mee voor aanbieders van telecommunicatienetwerken of -diensten. Voor zover een aanbieder *in het concrete geval* van een bevel administratie- of personele kosten heeft moeten maken, kan hij die bovendien op grond van artikel 13.6 lid 2 vergoed krijgen (zie onderdeel C), daargelaten de mogelijkheid om op grond van de Wet tarieven in strafzaken vergoeding van gemaakte kosten te claimen.
Onderdeel B van artikel III breidt de geheimhoudingsplicht die telecomaanbieders ingevolge artikel 13.5 Telecommunicatiewet hebben, uit tot gegevens met betrekking tot een bevel op grond van artikel 125i Sv.

**Artikel IV**

Wat het overgangsrecht betreft gelden, op enkele uitzonderingen na, de hoofdregels, dat wil zeggen ten aanzien van de wijzigingen in de strafbepalingen artikel 1 Sr en ten aanzien van de strafvorderlijke bepalingen het beginsel van onmiddellijke werking. Ook de wijzigingen van artikel 53, eerste lid, Sr hebben onmiddellijke werking. Dit betekent dat tussenpersonen die na inwerkingtreding van de wet voldoen aan de nieuwe voorwaarden niet kunnen worden vervolgd wegens (medeplichtigheid aan) een uitings- of verspreidingsdelict gepleegd vóór die inwerkingtreding.
Voor een aantal situaties is een bijzondere overgangsregeling getroffen. Onderdeel 1 van dit artikel stelt zeker dat gegevens uit het geautomatiseerd werk van een telecommunicatieaanbieder zoals e-mails, die voorafgaand aan inwerkingtreding van deze wet door een rechter-commissaris, een officier van justitie of een opsporingsambtenaar zijn vergaard, mogen worden geopend en ingezien óók als ze niet onder de restrictieve(re) voorwaarden van het nieuwe artikel 125n zouden vallen.

Onderdeel 2 ziet op het geval waarin aan bepaalde personen de verplichting kan worden opgelegd mee te werken aan het ontsleutelen van gegevensverkeer dat is afgetapt (artikel 126m, vijfde lid, Sv en 126t, vijfde lid, Sv). Dit bevel is gekoppeld aan de uitoefening van een andere bevoegdheid – de tapbevoegdheid – en kan in zoverre als accessoire bevoegdheid worden beschouwd. Gelet hierop brengt de rechtszekerheid mijns inziens mee dat, wanneer de tapbevoegdheid is uitgeoefend vóór inwerkingtreding van deze wet – op welk moment de (accessoire) medewerkingsverplichting nog niet bestond –, de betrokkene niet daarná alsnog tot medewerking aan de ontsleuteling van de verkregen gegevens kan worden gedwongen.
Onderdeel 3 ziet op de bevoegdheid tot «pseudokoop» van computergegevens door tussenkomst van een openbaar telecommunicatienetwerk en voorziet in de mogelijkheid om als het ware vooruit te lopen op de nieuwe regeling. Een dergelijke mogelijkheid is ook opgenomen in de Wet bijzondere opsporingsbevoegdheden. Een bevel dat materieel voldoet aan de voorwaarden gesteld in de artikelen 126i en 126q Sv, geldt vanaf inwerkingtreding van deze wet als een bevel in de zin van die artikelen.

De Minister van Justitie,
A. H. Korthals