Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2000–2001

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. 6

VERSLAG

Vastgesteld 21 september 2000

De vaste commissie voor Justitie[1] belast met het voorbereidend onderzoek van dit wetsvoorstel, brengt als volgt verslag uit van haar bevindingen.
Onder het voorbehoud dat de regering de gestelde vragen tijdig zal hebben beantwoord, acht de commissie de openbare behandeling van dit wetsvoorstel voldoende voorbereid.

ALGEMEEN

De leden van de PvdA-fractie kunnen de strekking van het wetsontwerp op hoofdlijnen ondersteunen. Wel betreuren zij het feit dat de bepalingen over de positie van providers geen onderdeel meer uitmaken van het wetsvoorstel. Zij zouden het op prijs stellen indien daar op korte termijn op enigerlei wijze toch voorzieningen voor worden getroffen. Kan de regering aangeven welke vorderingen er inmiddels op Europees gebied zijn gemaakt?
De internationale context geeft tegelijkertijd de beperkingen van dit wetsvoorstel aan. Het college van Procureurs-generaal weet dat in een treffend citaat te verwoorden in haar commentaar op het wetsvoorstel: «De grootste sta-in-de-weg hierbij en de achilleshiel van het gehele wetsvoorstel is de reikwijdte van de Nederlandse rechtsmacht.» Deelt de regering deze zienswijze en zo ja, welke internationale kansen en belemmeringen ziet de regering op dit gebied?
Hoe beziet de regering het gegeven dat internet-providers steeds grootschaliger en dus internationaler gaan opereren in de context van de reikwijdte van dit wetsvoorstel? De verticale concentratie van mediabedrijven duidt ook op een dergelijke ontwikkeling. Welke gevolgen hebben deze ontwikkelingen voor de nationale opsporingspraktijk?
Hoe beziet de regering het Amerikaanse voorstel om te komen tot een internationale cyberpolitie? Wat vindt de regering van de voorstellen van de Franse Minister Chevenement om snel te komen tot harmonisatie van wetgeving in de Europese unie op dit gebied? In welke fase bevindt zich de behandeling van het ontwerpverdrag van de Raad van Europa over computercriminaliteit? Vindt de Nederlandse regering zich terug in de daarin gehanteerde uitgangspunten of zijn er strijdigheden met voorliggend wetsontwerp?

[1] Samenstelling:
Leden: Swildens-Rozendaal (PvdA), Van de Camp (CDA), Biesheuvel (CDA), Scheltema-de Nie (D66), Zijlstra (PvdA), Kalsbeek-Jasperse (PvdA), Apostolou (PvdA), Middel (PvdA), Van Heemst (PvdA), voorzitter, Rouvoet (RPF), Rabbae (GroenLinks), Van Oven (PvdA), Kamp (VVD), Dittrich (D66), ondervoorzitter, O. P. G. Vos (VVD), Van Wijmen (CDA), De Wit (SP), Weekers (VVD), Wijn (CDA), Van der Staaij (SGP), Ross-van Dorp (CDA), Patijn (VVD), Niederer (VVD), Nicolaï (VVD), Halsema (GL).
Plv. leden: Wagenaar (PvdA), Balkenende (CDA), Verhagen (CDA), Van Vliet (D66), Duijkers (PvdA), Arib (PvdA), Kuijper (PvdA), Albayrak (PvdA), Barth (PvdA), Schutte (GPV), Karimi (GroenLinks), Santi (PvdA), Passtoors (VVD), Hoekema (D66), Van den Doel (VVD), Rietkerk (CDA), Marijnissen (SP), De Vries (VVD), Eurlings (CDA), Van Walsem (D66), Buijs (CDA), Rijpstra (VVD), Van Baalen (VVD), Van Blerck-Woerdman (VVD), Oedayraj Singh Varma (GroenLinks).

KST48047
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2000

De leden van de PvdA-fractie maken zich zorgen over het toegerust zijn van opsporingsambtenaren op het gebied van «cybercrime». Deze leden vragen hoe de zeven Interregionale bureaus digitale expertise inmiddels functioneren? Is daar cijfermateriaal over beschikbaar? Hoe staat het met om- en bijscholing van alle opsporingsambtenaren op digitaal gebied? In hoeverre wordt er samengewerkt met beveiligingsexperts uit het bedrijfsleven? Hoe beziet de regering de onwil bij het bedrijfsleven om gevallen van computercriminaliteit bij bevoegde instanties te melden? Gaat daardoor uiteindelijk ook niet een leereffect met bredere reikwijdte verloren?
Voorliggend wetsvoorstel richt zich vooral op cybercrime. Welke inzichten bestaan er inmiddels bij de regering over het voorkomen en bestrijden van cyberterrorisme, in het bijzonder daar waar dat tegen nationale overheden gericht zou kunnen zijn?
Met het juridisch beschermen van het e-mailgeheim is ervoor gekozen om vooruit te lopen op een grondwetsherziening van het huidige artikel 13. De leden van de PvdA-fractie vragen of hier in staatsrechtelijke zin wel de juiste weg wordt bewandeld. Juist nu behandeling van een dergelijke grondwetsherziening nabij is, zou er vanuit een oogpunt van zorgvuldigheid ook veel voor te zeggen zijn om eerst een grondwetswijziging te behandelen en vervolgens de desbetreffende organieke wetgeving.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Hoewel deze leden de hoofdlijnen van het wetsvoorstel onderschrijven, hebben zij nog een aantal opmerkingen.
In de memorie van toelichting wordt aangekondigd dat in de naaste toekomst nieuwe onderwerpen regeling behoeven, onder andere op grond van ontwikkelingen die nu nog onvoldoende zijn uitgekristalliseerd, zodat daarvoor nog geen voorziening kan worden getroffen, aldus de regering. Aan welke onderwerpen denkt de regering dan met name en op welke termijn verwacht de regering weer een nieuw wetsvoorstel?
In de Nota «wetgeving voor de elektronische snelweg» heeft de regering aangegeven dat het internationale karakter van het onderwerp zich niet goed verhoudt tot territoriaal georganiseerde overheden. Er zullen dus maatregelen op internationaal niveau genomen moeten worden. De regering vermeldt dat aan voorzieningen op het terrein van het internationale strafrecht en de internationale rechtshulp wordt gewerkt. Kan de regering aangeven op welke termijn ze de totstandkoming van het Cyberverdrag in het kader van de Raad van Europa verwacht?
Hoewel dit nieuwe wetsvoorstel een aantal onvolkomenheden in de huidige wet Computercriminaliteit corrigeert, zijn er nog een aantal aspecten waar het wetsvoorstel geen rekening houdt met ICT criminaliteit die voorzien kan worden. Ook houden de voorstellen naar de mening van de leden van de CDA-fractie onvoldoende rekening met de snelle convergentie tussen de telecommunicatiediensten en informatiediensten op bijvoorbeeld het internet. De computercriminaliteitwetgeving en de Telecommunicatiewet geven dan onduidelijke situaties, omdat er geen onderscheid gemaakt kan worden tussen de ISP's en de telecomoperators. (bijv. E-mail versus SMS). Kan de regering dit toelichten?
De leden van de CDA-fractie zouden graag van de regering een toelichting willen op het feit dat het inbreken in computernetwerken, hacken, niet strafbaar is gesteld in het wetsvoorstel. Dit terwijl dergelijke inbraken naar de mening van deze leden feitelijk computervredebreuk betekenen en hierdoor een basis voorhanden is voor ernstige computercriminaliteit.
In het kader van dit wetsvoorstel is gesproken over het invoeren van een kenteken ter bestrijding van computercriminaliteit. Kan de regering haar zienswijze hierop geven? Kan de regering in opiniërende zin een toelichting geven op het systeem dat in Engeland bestaat?

De leden van de D66-fractie hebben met interesse kennis genomen van het onderhavige wetsvoorstel. In het algemeen vragen deze leden of de

huidige ontwikkeling van de techniek met wetgeving valt bij te benen. Op welke termijn kan de Tweede Kamer het wetsvoorstel Computercriminaliteit III verwachten? Zijn er op dit moment reeds deelonderwerpen waarvoor voorzieningen zouden kunnen worden getroffen, die nu nog niet in het onderhavige wetsvoorstel Computercriminaliteit II staan vermeld?
Voorts zijn deze leden van mening dat de effectiviteit van het wetsvoorstel sterk afhankelijk is van de kennis en de technologische stand van zaken bij politie en het openbaar ministerie. Op dit punt hebben de leden van de D66-fractie zorgen. Uit het rapport «Cybercrime in Space» van enkele maanden geleden blijkt dat er sprake is van een gebrek aan kennis. Officieren van justitie en rechters weten zo weinig van computers en internet, dat strafzaken op dat terrein blijven liggen, zelfs wanneer het bewijs gemakkelijk te leveren is. Ook uit het actieprogramma «Digitaal rechercheren» is gebleken dat de ontwikkeling van digitaal rechercheren onvoldoende is.
Goederen kopen via het internet of betalen via de mobiele telefoon zijn nieuwe technieken die door criminelen worden toegepast en door politie en justitie zelden worden opgespoord dan wel vervolgd. Kan de regering ingaan op deze kritiek? Heeft elk regiokorps reeds een afdeling computercriminaliteit? Kan de regering een toelichting geven op het functioneren van de interregionale bureaus digitale expertise? Op welke wijze vindt de coördinatie plaats? Hoe wordt uitvoering gegeven aan de noodzaak tot specialisatie op dit terrein, zo vragen de leden van de D66-fractie.
In de memorie van toelichting valt te lezen dat van het politieapparaat mag worden verwacht dat het zich op de hoogte houdt van de informatietechnologische ontwikkelingen en mogelijkheden. De leden van de D66-fractie zijn het hiermee eens, maar vinden tevens dat de overheid hier een sturende rol moet spelen. Hoe wordt hier op dit moment aan voldaan?
In het verleden heeft de politie bepleit dat elke internetgebruiker een «kenteken» moet krijgen zodat zij niet langer anoniem kunnen blijven. Een dergelijk initiatief zou er voor moeten zorgen dat politie en justitie mensen die strafbare feiten plegen op de elektronische snelweg gemakkelijker kunnen achterhalen. Nu gebruikt men vaak een schuilnaam waardoor de opsporing ernstig bemoeilijkt wordt. Kan de regering ingaan op dit voorstel?
Tijdens de hoorzitting op 6 december 1999 in de Tweede Kamer werd er door meerdere sprekers op gewezen dat het onderhavige wetsvoorstel onvoldoende houvast biedt om cyberterreur en sabotage via het internet aan te pakken. Zo wordt er in het voorstel geen rekening gehouden met internationale terreuracties die via de elektronische snelweg worden uitgevochten. Kan de regering hier op ingaan? Op dezelfde hoorzitting werd gewaarschuwd dat personen die vanuit het buitenland aanslagen plegen niet strafrechtelijk kunnen worden aangepakt, met als gevolg dat deze personen ongestoord allerlei economische sectoren kunnen ontregelen, zoals we recentelijk zagen bij Homenet van ABN-Amro. Is de strafmaat voor hackers die in Nederland opereren niet aan de lage kant gezien de schade die men personen en bedrijven berokkent? Kan de regering hier nader op de strafmaat ingaan? Hoe is dit in andere landen geregeld?
In Amerika zijn het afgelopen jaar reeksen aanvallen van computerhackers op websites van grote bedrijven geweest. Door het sturen van grote hoeveelheden informatie over telefoonlijnen werden opstoppingen veroorzaakt, waardoor websites tijdelijk onbereikbaar werden. De Amerikaanse overheid heeft de bestrijding van computercriminaliteit tot prioriteit verheven. De Amerikaanse minister van Justitie noemde daarbij een paar aandachtsvelden zoals het vormen van een systeem waarbij computercriminaliteit snel gemeld wordt, het inlichten van locale overheden hoe ze op computercriminaliteit moeten reageren en het opleiden van personeel dat deze vorm van criminaliteit aanpakt en samenwerking met de industrie om de veiligheid te verbeteren. Welke voorbereiding treft de

Nederlandse regering om dergelijke aanvallen te voorkomen? Moet de overheid wellicht meer voorlichting gaan geven over computercriminaliteit? Is er überhaupt sprake van enige publieksvoorlichting?
Voorts wijzen de leden van de D66-fractie op Echelon, een omvangrijk elektronisch spionagenetwerk dat een groot deel van alle telefoongesprekken, faxen, e-mails en telexen onderschept. De ontwikkelaars van dit systeem schenden de mensenrechten door een ongeoorloofde inbreuk te maken op de privacy van burgers. Het bevreemdt deze leden dat hieraan in het wetsvoorstel geen aandacht wordt besteed, terwijl vanuit de Tweede Kamer toch al zesmaal in de afgelopen twee jaren vragen over dit spionagenetwerk zijn gesteld. In andere Europese landen lopen nu al geruime tijd onderzoeken naar Echelon. Waarom is er in Nederland tot op heden zo afwachtend gereageerd door de overheid als het gaat om Echelon? Kan de regering hier op ingaan?

Met grote belangstelling volgen de leden van de GroenLinks-fractie de ontwikkelingen op het gebied van de informatietechnologie en zijn dan ook verheugd te constateren dat de regering de nodige zorg besteed aan de totstandkoming van wetgeving die misbruik van deze ontwikkelingen zoveel mogelijk probeert tegen te gaan. De bestaande wetgeving loopt niet in de pas met de razendsnelle ontwikkelingen, die om een regelmatige en duidelijke koersbepaling vragen. De leden zijn zeer te spreken over het belang dat door de regering wordt gehecht aan het ontwikkelen van wetgeving die de technische ontwikkelingen kunnen blijven doorstaan. Met het oog hierop wordt betreurd dat de regering als gevolg van het uitblijven van een definitieve beslissing omtrent de Richtlijn elektronische handel heeft besloten de onderdelen A, T en U van onderdeel I van het wetsvoorstel te laten vervallen. Het is maatschappelijk immers van groot belang dat duidelijkheid ontstaat over de grenzen aan de aansprakelijkheid van elektronische tussenpersonen, niet in de laatste plaats omdat elektronische criminaliteit niet denkbaar is zonder tussenpersoon.

De leden van de SP-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij onderschrijven het streven van de regering de wetgeving in het verband met de voortschrijdende techniek aan te passen. Zij hechten daarbij aan waarborgen voor zekerstelling van de privacy.
De leden van de SP-fractie constateren dat in het wetsvoorstel te weinig aandacht wordt besteed aan de persoon van de systeembeheerder. De systeembeheerder (van grotere bedrijven, instellingen et cetera) heeft in zijn hoedanigheid nagenoeg onbeperkte toegang tot bestanden, gebruikerscodes en passwords. Hierdoor heeft deze persoon in principe onbeperkte toegang tot alle informatie die door medewerkers op een netwerk worden geplaatst. Kan de regering ingaan op de problematiek van de centrale figuur van de systeembeheerder en de mogelijkheden zonder een spoor na te laten eventueel informatie te vergaren door het gebruiken van de toegangscodes waarover deze beschikt? Dienen er in dit kader geen nadere eisen gesteld te worden aan de integriteit van deze figuur en dienen de controlemogelijkheden op zijn functioneren te worden vergroot? Acht de regering dit aspect niet een risico, bijvoorbeeld voor bedrijfsspionage?

Ook de leden van de SGP-fractie hebben met belangstelling van het wetsvoorstel kennisgenomen. Het wetsvoorstel biedt naar hun mening op diverse punten een zinvolle actualisering en verbetering van Computercriminaliteit-I. Niettemin hebben zij behoefte nog een aantal vragen met betrekking tot het wetsvoorstel aan de regering voor te leggen.

2. De aansprakelijkheid van tussenpersonen

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de verschillende onderdelen van voorliggend wetsvoorstel tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II). Een voorstel waaruit middels nota van wijziging een belangrijk onderdeel is geschrapt. De oorspronkelijk voorgestelde regeling van de strafrechtelijke aansprakelijkheid van tussenpersonen verschilt qua invalshoek en opzet met die van de Richtlijn elektronische handel. Met het kiezen voor het schrappen van de voorgestelde bepalingen en het treffen van een aparte regeling voor elektronische tussenpersonen, kiest de regering tevens voor uitstel van dit onderdeel. Dit terwijl regeling hiervan op korte termijn gewenst is. Kan de regering aangeven op welke termijn een aparte regeling voor de aansprakelijkheid van elektronische tussenpersonen kan worden verwacht? Niet duidelijk is of de regering met het kiezen voor een aparte regeling tevens zal kiezen voor een andere invalshoek en opzet. Is de regering van mening dat de mate van invloed op de inhoud van elektronische gegevens of diensten bepalend moet zijn voor de mate van aansprakelijkheid van tussenpersonen? Is hierbij voor de regering uitgangspunt dat een tussenpersoon alleen aansprakelijk is voor zover deze invloed heeft op de inhoud of de plaatsing van materiaal op de elektronische snelweg?
De leden van de VVD-fractie constateren dat ondanks het missen van een adequate regeling voor de aansprakelijkheid van tussenpersonen, het wetsvoorstel desondanks een aantal belangrijke ontwikkelingen in de informatiemaatschappij vertaalt naar het op orde brengen van de mate van bescherming, het inrichten van opsporingsbevoegdheden en het actualiseren van eerder ingevoerde bepalingen. Deze leden beoordelen de kwaliteit van het wetsvoorstel mede in het licht van de grote complexiteit van het onderwerp. Twee belangrijke kenmerken van de informatiemaatschappij zijn de toenemende snelheid waarmee deze zich ontwikkelt en het groeiend belang van internationale dimensies. Het wetsvoorstel bevat echter geen voorzieningen op het terrein van het internationale strafrecht en de internationale rechtshulp. Kan de regering, mede gezien de snelle ontwikkelingen op dit terrein, een actueel overzicht geven van richtlijnen, verdragen, afspraken, onderhandelingen en andere voorzieningen die zich richten op het terrein van de internationale aanpak van computercriminaliteit?

Nu de onderdelen die de aansprakelijkheid van tussenpersonen betreffen bij nota van wijziging van 13 april 2000 zijn komen te vervallen, zullen de leden van de GroenLinks-fractie daar te zijner tijd hun licht over laten schijnen. Zij kunnen instemmen met het voorstel het geschrapte artikel 53 te vervangen door een nieuwe aansprakelijkheidsregeling en met het besluit het onderhavige wetsvoorstel niet langer op te houden. Deze leden vernemen echter gaarne van de regering hoe er op dit moment wordt omgesprongen met het opsporen van daders van strafbare handelingen en met name in hoeverre tussenpersonen bereid zijn vrijwillig hun medewerking te verlenen aan het opsporen van bijvoorbeeld verspreiders van kinderporno.

De leden van de SP-fractie vragen de regering toe te lichten of de mogelijkheden verruimd moeten worden om muziek van extreemrechtse aard en de verspreiding daarvan via internet (zoals nordisc) tegen te gaan. In Nederland blijken volgens rapportage (KAFKA, *http://www.antifa.net/kafka*: artikel «justitie blundert bij vervolging Nazi-muziek») diverse distributeurs zich bezig te houden met het verspreiden van racistische, nazistische en antisemitische muzieksoorten, ook via Internet. In de laatste jaren zijn een aantal pogingen ondernomen de distributie van dit genre muziek

in Nederland aan te pakken, zonder al te veel succes. Kan de regering aangeven welke prioriteit er gelegd wordt in de bestrijding van dergelijke uitingen? Wat is de reactie op de constatering van Kafka dat Nederland in zekere zin een vrijplaats dreigt te worden voor distributeurs en op welke wijze wordt deze internethandel (met name vanuit de VS) in internationaal verband aangepakt?

De leden van de fracties van de RPF en het GPV hebben met belangstelling kennisgenomen van het onderhavige wetsvoorstel. Het wetsvoorstel is te beschouwen als een poging om de wetgeving aan te passen aan de snelle ontwikkelingen op de elektronische snelweg – zes jaar nadat de eerste wet computercriminaliteit een feit werd. Een van de uitgangspunten daarbij is geweest zoveel mogelijk parallellen na te streven tussen strafbare handelingen in het normale rechtsverkeer en handelingen in de digitale ruimte. Deze leden hechten er aan dit uitgangspunt te onderstrepen. Het internet is geen rechtsenclave, of «no-go-area». Te vaak is in het verleden met een zekere schroom gereageerd op dit uitgangspunt, met een beroep op het veronderstelde geheel eigen karakter van de digitale snelweg.
Een ander uitgangspunt is dat de wetgeving zo «techniek» neutraal mogelijk moet worden geformuleerd. Is dit doel behaald? Zij vragen dit in het bijzonder in het licht van de opmerking in de memorie van toelichting, dat in de naaste toekomst nieuwe onderwerpen een regeling behoeven. Over welke onderwerpen gaat dat dan? Op welke termijn is nieuwe regeling naar verwachting aan de orde?
De wetgeving liep aanvankelijk voorop op voorziene Europese regelgeving, maar de Richtlijn waar het hier om gaat is nog steeds niet definitief vastgesteld. Dit is reden waarom een belangrijk onderdeel, namelijk de aansprakelijkheid van tussenpersonen, uit het wetsvoorstel is gelicht. De leden van de fracties van de RPF en het GPV betreuren het vervallen van dit onderdeel, alsmede het vooralsnog ontbreken van een poging om bij nota van wijziging een onderdeel in het wetsvoorstel te voegen dat beter overeenstemt met de veronderstelde inhoud van de richtlijn.
De leden van de fracties van de RPF en het GPV vragen in het verlengde hiervan of het noodzakelijk is om het geheel van de onderdelen A, T en U te laten vervallen. In het bijzonder vragen zij of er een regeling gemist kan worden, zoals in artikel 53 voorzien, waarmee de tussenpersoon van de zijde door het OM kan worden gemaand om maatregelen te treffen om verdere verspreiding van het materiaal te voorkomen. Is het juist dat bij vervallen van die bepaling, alleen medewerking kan worden afgedwongen die betrekking heeft op het verzamelen van gegevens in het kader van de waarheidsvinding op basis van een gerechtelijk vooronderzoek ex artikel 125i Sv?
Tevens vragen deze leden in hoeverre artikel 53 oud bij een eventuele gerechtelijke procedure al dan niet via een extensieve interpretatie geacht kan worden van belang te zijn bij de vraag in hoeverre een internetprovider mede aansprakelijk moet worden geacht bij de verspreiding van strafbaar materiaal.

In het wetsvoorstel wordt de lijn gekozen het briefgeheim in beginsel onverkort door te trekken naar de beveiliging van e-mail. Aan de ene kant kunnen de leden van de fracties van de RPF en het GPV hiervoor begrip opbrengen, gezien de functie van e-mail in de maatschappij. Wel vragen zij zich af of de context van het medium niet zou moeten leiden tot een zekere risicoaanvaarding, er van uitgaande dat het briefgeheim op de elektronische snelweg op papier wel geregeld kan worden maar praktisch gezien de nodige voeten in de aarde heeft. Hoe ver gaat de verantwoordelijkheid van een provider om gegevens te beschermen tegen bijvoorbeeld hackers?

De leden van de fracties van de RPF en het GPV vragen voorts of de regeling in het wetsvoorstel er afdoende rekening mee houdt dat een ISP in het kader van wat je de bezorgplicht zou kunnen noemen, wel eens kennis moet nemen van de inhoud van in eerste instantie niet af te leveren e-mail.

Allereerst noemen de leden van de SGP-fractie de in het derde lid van artikel 53 Sr. vervatte omschrijving van een tussenpersoon. Daaruit blijkt dat alleen professioneel of bedrijfsmatig handelende tussenpersonen kunnen profiteren van de regeling van niet-vervolgbaarheid. Zij vragen waarom de uitsluiting van niet-professionele tussenpersonen in de memorie van toelichting niet wordt gemotiveerd, terwijl dit evenmin uit de ratio van de regeling lijkt voort te vloeien. Wordt de bescherming van aanbieders die verspreiden zonder commercieel oogmerk of voor wie het verspreiden niet de hoofdactiviteit is, zo niet onnodig ingeperkt?
Zij vragen voorts of een internetaanbieder die moet volstaan met het noemen van de anonimiseerder van berichten die van hun bron-aanduiding zijn ontdaan als dan niettemin aanspraak zal kunnen maken op de bescherming van artikel 53.
Deze leden hebben ook een vraag bij de voorwaarde voor niet-vervolgbaarheid, namelijk dat de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan alle handelingen dient te verrichten die redelijkerwijs van hem gevergd kunnen worden ter voorkoming van verdere verspreiding van het bericht. Als de gewraakte uiting evident strafbaar is, zal de internetaanbieder deze ook wel zonder aanmaning weghalen. Als echter niet op voorhand duidelijk is dat de uiting strafbaar is, is het dan op voorhand logisch dat de uiting verwijderd moet worden zonder dat daar een rechterlijke uitspraak aan ten grondslag ligt, zo vragen de leden van de SGP-fractie. Wordt in het voorgestelde systeem de officier van justitie niet te gemakkelijk uitgenodigd om ook in twijfelachtige gevallen een aanmaning tot verwijdering naar de Internetaanbieder te doen uitgaan? Deze leden vragen daarom of deze voorwaarde geen heroverweging verdient, gezien ook de bevoegdheden die de officier van justitie zelf heeft om verdere verspreiding te voorkomen.
De voorgestelde tekst van artikel 53 Sr. behoudt de oude formulering, maar breidt deze (slechts) uit door naast de drukpers enig ander middel voor de openbaarmaking of verspreiding van uitingen in woord, beeld of geluid te noemen. Betekent dit, zo vragen deze leden, dat het voorgestelde artikel 53 Sr. betrekking heeft op dezelfde delicten als vanouds. In de memorie van toelichting wordt over de delicten niets gezegd, in het bijzonder niet dat enige afwijking van het geldende recht is beoogd. Als dat zo is, kunnen zich dan bijvoorbeeld geen problemen voordoen wanneer de internetaanbieder die als tussenpersoon optreedt, constateert dat reclame gemaakt wordt voor verdovende middelen of het aanbieden van gokspelen zonder vergunning. Moet aangenomen worden dat de regeling, gezien de ratio ervan (bescherming van uitingen), in deze gevallen niet van toepassing is?

3. Vernietiging van computergegevens

De leden van de PvdA-fractie juichen de voorgestelde uitbreiding van bevoegdheden toe. Wel vragen zij of het juist is, zoals wordt gesteld, dat de vermogenswaarde van gegevens vaak ontbreekt dan wel moeilijk te kwantificeren is. Juist in het economische verkeer neemt de waarde van bijvoorbeeld klantgegevens steeds meer toe. Zij vragen dan ook of hier toch niet een aparte wettelijke voorziening voor dient te worden getroffen al dan niet in relatie met de wet Economische Delicten.
In de memorie van toelichting wordt een wel erg eng begrip van e-mail opgevoerd, namelijk als verkeer tussen twee personen. De praktijk leert

inmiddels dat e-mails vaak aan meerdere personen tegelijkertijd worden gestuurd en door ontvangers ook regelmatig worden doorgezonden. Zou de regering in het licht van deze opmerkingen willen aangeven of dan de voorwaarden voor het ontoegankelijk maken en voor vernietiging nog steeds gelden? Zou ook een duidelijkere grens kunnen worden aangegeven als de verspreiding van e-mail in kwantitatieve zin wordt belicht?

De vernietiging van computergegevens vormt een inbreuk op de rechten van belanghebbenden. Waar «off-line» geldt dat een dergelijke inbreuk gerechtvaardigd kan zijn uit hoofden van een opsporings- en handhavingsbelang, geldt wat betreft de leden van de VVD-fractie hetzelfde «on-line». Deze leden zijn met de regering van mening dat er een lacune bestaat in de beslagleggingbevoegdheden waar het gaat om gegevens die deel uitmaken van een strafbaar feit of met behulp waarvan een strafbaar feit is begaan. Zij vragen of de voorgestelde bepalingen deze lacune in voldoende mate afdichten. Welke gegevens die zijn vastgelegd bij onderzoek in geautomatiseerde werken, hoeven niet te worden vernietigd nadat zij van geen betekenis meer zijn voor het onderzoek? Worden bij een dergelijk onderzoek ook kopieën gemaakt die niet ten behoeve staan van justitie? De Hoge Raad heeft bevestigd dat gegevens geen goed zijn. Hierdoor bieden bestaande inbeslagnamebevoegdheden onvoldoende mogelijkheden om gegevens in beslag te nemen. Dit is alleen anders indien de gegevens nauw verbonden zijn aan een goed dat wel in beslag kan worden genomen. Dit is het geval bij bijvoorbeeld een diskette. Deze leden vragen uit het oogpunt van proportionaliteit, of dit ook geldt voor een al dan niet verwisselbare harde schijf. Is hierbij van belang of de harde schijf tevens het besturingsprogramma en/of applicaties bevat?
De vraag of de voorgestelde bepalingen de geconstateerde lacune in voldoende mate afdichten hangt grotendeels af van de praktische hanteerbaarheid. De maatregelen van het ontoegankelijk maken en de vernietiging zijn mede bestemd voor toepassing in openbare, internationale netwerken. Betekent dit dat ook computers in het buitenland kunnen worden onderworpen aan deze maatregelen of is toepassing alleen mogelijk op Nederlandse computers en dan onafhankelijk van de vraag of deze laatste zich in een nationaal of internationaal netwerk bevinden, dan wel stand-alone machines zijn? Ook is het de vraag voor wie de gegevens allemaal ontoegankelijk moeten worden gemaakt. Hoe kunnen in praktische zin gegevens voor de netwerkbeheerder ontoegankelijk worden gemaakt, anders dan door fysieke verwijdering, nu deze netwerkbeheerder uit hoofde van zijn functie volledige toegangsrechten kent. Is een dergelijke ontoegankelijkmaking ook voorstelbaar indien het problemen oplevert voor het functioneren van het netwerk als zodanig?
De regering verwacht van het politieapparaat dat het zich op de hoogte stelt van de informatietechnologische ontwikkelingen en mogelijkheden die nodig zijn om een effectieve inzet van de voorgestelde bevoegdheden te realiseren. Toch constateert de regering ook dat het wetsvoorstel niet tot aanvullende eisen met betrekking tot de organisatie, uitrusting of opleiding van politie of justitie leidt. De leden van de VVD-fractie vragen of er nu wel of niet een investering in de capaciteit van het politieapparaat nodig is? Een tekort aan kennis kan worden opgevangen met behulp van de inschakeling van externe deskundigen. Zaak is dan wel de vertrouwelijkheid van het onderzoek te garanderen. Welke garanties biedt het voorliggende voorstel voor de vertrouwelijkheid van het onderzoek? Een probleem bij de ontoegankelijkmaking en vernietiging van gegevens is de zeer korte tijdspanne waarbinnen gegevens kunnen worden gekopieerd naar een andere gegevensdrager die niet op dat zelfde moment toegankelijk is voor politie of justitie. Dit betekent dat terwijl aan de ene kant gegevens ontoegankelijk worden gemaakt, zij aan de andere kant aan de controle van politie en justitie kunnen worden onttrokken. Is het wenselijk om in dergelijke gevallen het bevel te kunnen uitvaardigen om alle bewer-

king, opslag of overdracht van gegevens te staken? De racistische uiting gevonden in een e-mail-box is op zichzelf nog geen grond om de betrokken gegevens ontoegankelijk te maken. Is dit anders indien de uiting is verzonden aan een groep van personen of aan een openbare mailinglist?

De leden van de CDA-fractie stellen dat over het vernietigen van printergegevens en van de telefoontap reeds uitspraken van het Europese Hof (Zaak Edwards vs UK-16–12–92), van het Hof Amsterdam (NJ 1994, no 709& 710) en van de Hoge Raad (27-06-1995) bekend zijn. Daaruit blijkt dat betreffende gegevens niet eerder vernietigd mogen worden, dan nadat de verdediging voldoende gelegenheid heeft gehad om een verzoek in te dienen om een of meer gegevens in het belang van de verdediging aan de processtukken toe te voegen. Deze lijn in de jurisprudentie en in het wetsvoorstel met betrekking tot de telefoontap, zouden ook geprojecteerd kunnen worden op artikel 125n Sv. Hierin wordt voorgesteld om de gegevens pas op zijn vroegst een maand na de definitieve rechterlijke uitspraak te vernietigen. Dit zou praktisch neerkomen op het bewaren van gegevens, totdat er voor de verdachte geen rechtsmiddelen meer openstaan. Ter voorkoming van misverstanden zou hier meer duidelijkheid gewenst zijn.
Het nieuwe artikel 125o Sv geeft aan de officier van justitie of de rechter-commissaris de bevoegdheid om te bepalen dat computergegevens met behulp waarvan het strafbaar feit is gepleegd ontoegankelijk worden gemaakt. Naar het oordeel van het College van Procureurs-generaal behoort de rechter-commissaris geen zeggenschap te hebben over beëindiging van het strafbare feit of over de voorkoming van nieuwe strafbare feiten. Dit behoort niet tot de taken van de rechter-commissaris. Wat is de reactie van de regering hierop?
Het zou volgens de leden van de CDA-fractie wenselijk zijn dat de wetgever nadere waarborgen en randvoorwaarden geeft voor onderzoek in een complexe geautomatiseerde omgeving, zoals een rekencentrum. Weliswaar gelden bij een dergelijk onderzoek de algemene beginselen van proportionaliteit en subsidiariteit, maar gezien de risico's voor buitenproportionele schade bij onoordeelkundig gebruik van bevoegdheden, dient de wetgever naar onze mening speciale waarborgen te creëren. De leden van de D66-fractie vinden de justitiële bevoegdheid tot het ontoegankelijk maken en/of vernietigen van computergegevens een belangrijke nieuwe voorziening. In artikel 125o Sv wordt bepaald dat de officier van justitie en de rechter-commissaris de bevoegdheid hebben 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 strafbare feit of ter voorkoming van nieuwe strafbare feiten. Kan de regering beargumenteren waarom de rechter-commissaris zeggenschap moet hebben over de beëindiging van het strafbare feit of over voorkoming van nieuwe strafbare feiten? Behoort dit tot de taken van de rechter-commissaris?
Voor ontoegankelijkmaking zal in sommige gevallen de medewerking van de netwerkbeheerder noodzakelijk zijn. De beheerder kan daarvoor eventueel een vergoeding krijgen op basis van de wet tarieven in strafzaken? Waar hangt het vanaf of een beheerder aanspraak kan maken op een vergoeding?

De leden van de GroenLinks-fractie stellen dat de informatietechnologie het afgelopen decennium een enorme vlucht heeft genomen. Meer dan ooit is in het dagelijks leven merkbaar dat computers een niet meer weg te denken rol spelen in de samenleving. De angst voor de millenniumbug heeft velen doen beseffen dat de betrouwbaarheid van de informatietechnologie van vitaal belang kan zijn voor het continueren van het persoonlijk

en het openbaar leven. Hiermee is het belang van een deugdelijke bescherming van de digitale snelweg aangetoond. Waar grote belangen op het spel staan, dient zich haast als vanzelfsprekend ook de criminaliteit aan.
In de huidige regelgeving betreffende computercriminaliteit zijn door de stand van de techniek grote lacunes ontstaan, onder meer door het ontbreken van mogelijkheden tot inbeslagname en vernietiging van computergegevens. Indien in een geautomatiseerd werk gegevens worden aangetroffen die op enige wijze samenhang vertonen met een strafbaar feit, bestaat thans slechts de mogelijkheid voor de politie om een kopie te maken. Inbeslagname en vernietiging is niet mogelijk, aangezien gegevens geen goed zijn. De leden van de GroenLinks-fractie zijn met de regering van oordeel dat in deze tekortkoming dient te worden voorzien.
In het voorgestelde artikel 125o Sv krijgt de officier van justitie, of tijdens het GVO de rechter-commissaris, de bevoegdheid te bepalen dat computergegevens met betrekking tot welke of met behulp waarvan een strafbaar feit is gepleegd, ontoegankelijk worden gemaakt. Waar telkens de vergelijking wordt getrokken met huiszoeking en inbeslagname, zijn de leden van de GroenLinks-fractie van oordeel dat het tijdelijk onbruikbaar maken van de toegangspoort van een computer een te vérgaande maatregel is. De te nemen maatregel dient zoveel mogelijk beperkt te blijven tot dát deel van de bestanden waarop het strafbare feit(en) betrekking heeft en niet de vrijheid van meningsuiting verder te beperken dan noodzakelijk. Daar komt bij dat het onbruikbaar maken van de toegangspoort van een computer in bepaalde gevallen schade kan veroorzaken die niet altijd is te voorzien en wellicht in aanmerking zal komen voor vergoeding door de Staat. Dit dient te worden voorkomen, menen deze leden. Is het niet beter om het ontoegankelijk maken van computergegevens te beperken tot die gegevens die samenhang vertonen met het strafbare feit?
De leden van de GroenLinks-fractie vinden het van belang dat de notificatieplicht als bedoeld in het voorgestelde artikel 125p Sv niet wordt beperkt tot de in lid drie omschreven personen. Er zou, naar zij menen, meer ruimte gelaten moeten worden voor een grotere groep personen, aangezien ook voor anderen dan de in lid 3 genoemde personen artikel 13 EVRM kan gelden. Een ieder wiens rechten en vrijheden zijn geschonden, heeft recht op een «effective remedy». Het is immers zeer goed denkbaar dat de privacy van een bekende persoon is geschonden door een onderzoek, zonder dat deze persoon hier weet van krijgt en dus geen «effective remedy» heeft voor een nationale

4. Medewerking aan de ontsleuteling van gegevens

Medewerking aan de ontsleuteling van gegevens zal vanwege het nemoteneturbeginsel niet worden bevolen aan verdachten. Dit brengt met zich mee dat alleen indien via een derde ontsleuteling mogelijk is, een bevel tot medewerking aan ontsleuteling kan bijdragen aan de opsporing. Hoe kan worden bevorderd dat specifieke derden zoals TTP's, vaker over voldoende kennis beschikken om ontsleuteling mogelijk te maken? Is het in dit verband wenselijk om een sleuteldeponeringsverplichting te introduceren. De leden van de VVD-fractie vragen of de medewerkingverplichting in voldoende mate kan worden afgedwongen bij een weigerachtige derde. Is de sanctie die rust op het niet voldoen aan een ambtelijk bevel ook toepasbaar bij een weigerachtige derde? Is de regering van mening dat deze sanctie in verhouding staat tot het soms aanwezige grote belang om niet mee te werken? Ook vragen deze leden of de medewerkingverplichting onder omstandigheden een afbreuk kan doen aan de bewijskracht van het ontsleutelde materiaal. Is altijd zeker dat de gegevens waarvan ontsleuteling is bevolen daadwerkelijk ook worden ontsleuteld?

Is voorstelbaar dat er bijvoorbeeld een speciaal voor dat doeleinden opgeslagen bestand wordt ontsleuteld dat ongemerkt in de plaats treed voor de eigenlijke gewenste gegevens? Hoe kan met zekerheid worden aangetoond dat iets dergelijks niet plaatsvindt? Is dit gevaar groter indien de derde zelf de ontsleuteling verzorgt? Hoe moet in dit licht worden beoordeeld dat de derde zelf kan beoordelen of hij de sleutel afstaat dan wel zelf de ontsleuteling verzorgt? Is hier een rol weggelegd voor een deskundige derde partij?
Het bevel tot ontsleuteling kan niet langer alleen bij de doorzoeking plaatsvinden maar kan na invoering van het voorliggende wetsvoorstel, ook terstond daarna plaatsvinden. De leden van de VVD-fractie begrijpen dat deze tijdsuitbreiding noodzakelijk is voor een effectieve inzet van deze maatregel. Is er echter niet gekozen voor een te beperkte uitbreiding? Immers, de bevoegdheid blijft net als die van het bevel tot toegangsverschaffing gekoppeld aan de doorzoeking? Elders wordt wel aansluiting gezocht bij alle gevallen van onderzoek in een geautomatiseerd werk. Geniet het vanuit overwegingen van praktische hanteerbaarheid en een grotere rechtsconsistentie niet de voorkeur om dit ook het uitgangspunt te laten zijn bij de onstleuteling en de toegangsverschaffing?

In het wetsvoorstel wordt een medewerkingverplichting voor de verdachte aan de ontsleuteling van opgeslagen of stromende gegevens geïntroduceerd, stellen de leden van de CDA-fractie. De regering acht het onder omstandigheden (ernstige bezwaren en dringende noodzakelijkheid) gerechtvaardigd een daartoe strekkend bevel te richten tot de verdachte. Terecht constateert de regering dat het Nederlandse strafrecht geen onvoorwaardelijk recht of beginsel kent dat de verdachte op enigerlei wijze kan worden verplicht mee te werken aan de bewijsgaring jegens hemzelf. In dat verband wordt onder andere gewezen op de verplichting DNA onderzoek te ondergaan. De regering haalt een uitspraak aan van het Europese Hof voor de rechten van de mens in de Zaak Saunders (EHRM 17 dec 1996). Kan de regering ingaan op de gesuggereerde spanning tussen de voorgestelde verplichting tot actieve medewerking door de verdachte en de uitspraak in de zaak Saunders, waar de nadruk wordt gelegd op de «will of the accused person to remain silent». Juist het feit dat in het wetsvoorstel een actieve handeling van de verdachte wordt geëist, te weten het medewerking verlenen aan ontsleuteling door kennis ter beschikking te stellen of de versleuteling ongedaan te maken, maakt dat sprake is van een heel andere situatie dan bij het gedogen van een adem-, bloed-, urine-, of DNA onderzoek, waarbij de verdachte hoofdzakelijk gedoogt, maar niet actief hoeft te spreken of mee te werken. Juist door deze voorgestelde dwang tot spreken of meewerken, waardoor de «will of an accused person to remain silent» wordt genegeerd, maakt dat de grens van het uitoefenen van toelaatbare dwang wordt overschreden. Wat is de reactie van de regering op de vraag of hier niet een kritische grens wordt gepasseerd, waardoor de deur wordt opengezet voor het in de wet opnemen van vele andere vormen van verplicht meewerken door de verdachte (bijvoorbeeld het meewerken aan het begrijpelijk maken van in telefoongesprekken gebruikte codewoorden, het noemen van kluis- of rekeningnummers etc.). Wat niet duidelijk is in dit artikel is wie het bevel kan geven en welke procedure moet worden gevolgd. Zoals het nu geformuleerd is komt het er op neer dat de bescherming van de eigen «cyber» levenssfeer niet wordt gerespecteerd, maar uitsluitend als opsporingsprobleem wordt gezien. De vergelijking met huiszoeking (als meest vergaande bevoegdheid in ons wetboek van strafvordering) dringt zich hier op en gelijksoortige waarborgen lijken daarom nodig.
Artikel 126 voorziet in de mogelijkheid dat de houder niet de sleutel ter beschikking stelt, doch deze zelf hanteert om het versleutelde signaal te ontcijferen. Dit betekent dat het systeem afhankelijk is van de medewerking en de betrouwbaarheid van degene die de gegevens moet ontsleu-

telen. Het is denkbaar dat de betrokkene hele andere gegevens verstrekt. Hoe vindt het toezicht op de ontsleuteling plaats? Overwogen zou kunnen worden om een buiten de commercialiteit gezochte gerechtelijk deskundige de ontsleuteling in samenwerking met de sleutelhouder ter hand te laten nemen. Het gerechtelijk laboratorium zou dit bijvoorbeeld voor zijn rekening kunnen nemen.
Verwacht de regering dat de strafbedreiging van artikel 184 (weigering te voldoen aan een ambtelijk bevel) voldoende soelaas biedt als de betrokkene weigert om aan de verplichting tot ontsleuteling te voldoen? Denkt de regering niet dat deze strafbedreiging te gering is in verhouding tot het belang dat betrokkene kan hebben bij een mislukte gegevensverstrekking?

Het wetsvoorstel voorziet in een medewerkingsverplichting van derden bij het ontsleutelen van gegevensverkeer. De voorgestelde bepaling voorziet echter in de mogelijkheid dat de houder, naar zijn keuze, niet de sleutel ter beschikking stelt, doch deze zelf hanteert om het versleutelde materiaal te ontcijferen. Dit betekent naar de mening van de leden van de D66-fractie dat het systeem afhankelijk is van de medewerking en de betrouwbaarheid van degene die de gegevens moet ontsleutelen. Is het niet denkbaar dat de betrokkene hele andere gegevens verstrekt? Klopt het dat er dan niet met zekerheid kan worden gezegd dat ook daadwerkelijk de versleutelde gegevens zijn verstrekt? Met andere woorden, de bewijsketen is op deze wijze niet geheel gesloten. Het voorgestelde systeem is afhankelijk van de medewerking en betrouwbaarheid van de ontsleutelaar. Is dit wenselijk? Hoe vindt het toezicht op de ontsleuteling plaats? Heeft de regering overwogen een buiten de commercialiteit gerechtelijke deskundige de ontsleuteling in samenwerking met de sleutelhouder ter hand te laten nemen?
Verwacht de regering dat de stafbedreiging van artikel 184 Sr (weigering te voldoen aan een ambtelijk bevel) voldoende soelaas biedt indien de betrokkene weigert om aan de verplichting tot onsleuteling gehoor te geven? Is deze strafbedreiging in verhouding tot het belang dat de betrokkene kan hebben bij mislukte gegevensverstrekking? Is de impuls om mee te werken groot genoeg, zo vragen de leden van de D66-fractie?
Het is overwogen om het mogelijk te maken dat een bevel tot medewerking aan de onsleuteling van gegevens ook tot de verdachte zou kunnen worden gericht. Uiteindelijk vond de regering dit een stap te ver gaan. In de wetenschappelijke wereld zijn de meningen over dit onderwerp verdeeld. Volgens sommigen is het niet in strijd met het nemo-teneturbeginsel om de verdachte bij wet te verplichten de sleutel tot een encryptieprogramma te verstrekken. Het nemo-teneturbeginsel ziet namelijk hoofdzakelijk op de verklaringsvrijheid van de verdachte en niet op de eisen van medewerking van de verdachte aan de verkrijging van materiaal dat onafhankelijk van zijn wil bestaat. Met betrekking tot dit laatste stelt de regering in de memorie van toelichting dat daarvan bij een door de verdachte zelf gekozen en slechts in zijn geheugen opgeslagen wachtwoord geen sprake is. De leden van de D66-fractie zijn hier niet geheel van overtuigd. Onafhankelijk van de wil van de verdachte bestaat het materiaal namelijk wel, alleen bestaat er geen toegang tot het materiaal. Kan de regering hier nader op ingaan?

De leden van de GroenLinks-fractie zijn met de regering van oordeel dat het verplichten van de verdachte tot medewerking aan ontsleuteling van gegevens een stap te ver gaat. Het zwijgrecht is een zodanig zwaarwegend recht, dat een bevel tot medewerking slechts aan derden kan worden verstrekt. Deze leden stellen het op prijs dat de regering dit expliciet in de artikelen 126m, zesde lid, en 126t, zesde lid, Sv van het wetsvoorstel heeft opgenomen.
Desalniettemin twijfelen deze leden aan de effectiviteit van de voorgestelde regeling. Het is een aardige gedachte dat bij de ontsleuteling van

bepaalde gegevens de medewerking nodig is van diegene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van telecommunicatie, maar in de praktijk kan dit op een probleem stuiten waarvan in de memorie van toelichting niet blijkt dat de regering daar aan heeft gedacht.
Wanneer de sleutel tot de gegevens in handen is van een TTP (Trusted Third Party) worden geen grote problemen verwacht, want zij zullen over het algemeen geen enkel persoonlijk belang hebben om geen medewerking te verlenen. Anders ligt het echter indien die derde de ontvanger is van een versleuteld e-mailbericht, dat door de verdachte aan hem is verstuurd. Indien uit het bericht namelijk zou blijken dat de ontvanger zich eveneens schuldig zou maken aan het plegen van een strafbaar feit, dan wordt hij gedwongen mee te werken aan zijn eigen verdachtmaking. Ten tijde van het bevel is hij immers nog geen verdachte en kan zich niet beroepen op het zesde lid van de artikelen 126m en 126t Sv. Hoe verhoudt zich dit met de algemene strafrechtsbeginselen? Is de regering bereid de positie van deze derde nader toe te lichten? Is het wellicht zo dat deze derde zich eveneens op het zesde lid van de artikelen 126m en 126t Sv kan beroepen? Het hier omschreven probleem klemt temeer nu de verwachting is dat veel vaker de medewerking aan ontsleuteling van deze ontvanger van berichten nodig zal zijn dan de medewerking van een TTP.

5. Het onderscheid tussen opgeslagen en stromende gegevens

In de memorie van toelichting wordt het onderscheid tussen opgeslagen gegevens en gegevens in transport aangegeven. De leden van de PvdA-fractie missen substantiële onderbouwing voor het handhaven van dit onderscheid. Zou de regering met een aantal voorbeelden uit de dagelijkse praktijk van de opsporing kunnen pogen dit onderscheid te onderbouwen? De leden van de PvdA-fractie vrezen dat men in de dagelijkse opsporingspraktijk steeds lastiger met het gemaakte onderscheid uit de voeten kan. Zij vragen bovendien of het gehanteerde onderscheid tussen onderzoek naar reeds bestaande gegevens en onderzoek gedurende zekere tijd naar gegevens die op het moment van aanvang van het onderzoek nog niet bestaan, de wet niet nog onnodig ingewikkelder en lastiger te hanteren maakt.

De regering kiest ervoor om het bestaande onderscheid tussen opgeslagen en stromende gegevens te handhaven. Dit onderscheid moet worden gehandhaafd omdat alternatieve termen alleen in ruimere, abstractere bewoordingen kunnen worden gevat. De regering is van mening dat de gehanteerde terminologie goed aansluit bij de maatschappelijke werkelijkheid en het normale spraakgebruik. De leden van de VVD-fractie vragen of deze constatering juist is. Enerzijds schets de regering zelf een aantal voorbeelden waarbij het gehanteerde onderscheid minder duidelijk is. Ook geeft zij aan dat het gehanteerde onderscheid wellicht minder essentieel is dan in het verleden werd gedacht. Tenslotte, en meest belangrijk, langzamerhand wordt het gehanteerde onderscheid meer en meer begrepen als een onderscheid tussen bestaande en toekomstige gegevens. Onderschrijft de regering deze laatste trend en ziet zij hierin een oplossing voor de door verschillende instanties geconstateerde vervaging van het huidig gehanteerde onderscheid? Voorts merken deze leden op dat naar hun mening de algemene regel van geen geheimhouding bij onderzoek naar bestaande gegevens, vaker dan in de geschetste gevallen, doorbreking behoeft. Met één druk op de knop zijn in geautomatiseerde systemen opgeslagen gegevens te verwijderen. Het bekend worden van een onderzoek naar die gegevens kan op die wijze eenvoudig gefrustreerd worden. Welke bevoegdheden hebben politie en justitie nodig om ook in dergelijke gevallen het onderzoek in het geheim te mogen uitvoeren?

Het voorstel handhaaft het verschil in benadering van opgeslagen en stromende e-mail. Bij e-mail in transport wordt aangesloten bij het regime van het aftappen van telecommunicatie. Bij opgeslagen e-mail wordt een vergelijkbare bescherming met traditionele post gemaakt. Dit brengt met zich mee dat het toepassen van opsporingsmaatregelen ten opzichte van opgeslagen e-mail aan strengere voorwaarden is verbonden dan bij e-mail in transport. De leden van de VVD-fractie zijn op voorhand nog niet overtuigd van de noodzaak van een dergelijk onderscheid. Voor hen speelt het argument dat de opsporing wordt bezwaard met een aantal extra voorwaarden hierbij een belangrijke rol. Ook zien zij zowel bij e-mail in transport als bij opgeslagen e-mail een grote feitelijke overeenkomst tussen het aftappen van telecommunicatie en het aftappen van e-mail. In beide gevallen wordt met de tap een kopie gemaakt van het oorspronkelijke bericht. Het oorspronkelijke bericht wordt zowel bij de telefoontap als de e-mail tap ongestoord doorgevoerd naar de ontvanger. Dit geldt ook voor het opgeslagen bericht. Deze kan immers worden uitgelezen zonder dat eigenaar hiervan kennis neemt. Dit in tegenstelling tot de opengescheurde envelop. Kan de regering aangeven waarom het verkozen onderscheid geen verzwaring van de voorwaarden betekent ten opzichte van de situatie waarbij in zijn geheel wordt aangesloten bij de systematiek van het aftappen van telecommunicatie?

In de Nota «Wetgeving voor de elektronische snelweg» wordt aandacht besteed aan de begrippen transport en opslag. Van opslag is sprake, als gegevens kunnen worden geraadpleegd op een door de mens te bepalen tijdstip. Van transport is sprake als gegevens zich in een toestand van telecommunicatie bevinden. Het onderscheidend criterium is dus of een gegeven te raadplegen is op een door de mens te bepalen tijdstip. Is in het wetsvoorstel ook uitgegaan van dit criterium, zo vragen zowel de leden van de CDA-fractie als de leden van de D66-fractie. Verwacht de regering dat het onderscheid tussen het strafvorderlijk onderzoek van gegevens opgeslagen in de computer en het onderscheppen van gegevens tijdens het transport, voor de praktijk voldoende duidelijk is? Zijn alle knelpunten die zich in het verleden op dit terrein hebben voorgedaan, opgelost?
Hoewel in het wetsvoorstel terecht wordt uitgegaan van een scheiding tussen opgeslagen of huidige gegevens en stromende of toekomstige gegevens, wordt er onvoldoende bescherming geboden met betrekking tot het inzien van e-mail, dat net zoals ongeopende post in de off-line wereld extra bescherming verdient. In de artikelen 125i en 125n wil de regering een onderscheid maken tussen het uitleveren van post c.q. opgeslagen e-mail (net als bij de artikelen 100 en 101 Sv) en anderzijds het inzien van ongeopende post c.q. ongeopende en niet opgehaalde e-mail waarvoor een extra bevel en afweging van de rechter-commissaris nodig is. Uitlevering van e-mail kan echter technisch alleen maar «geopend». Daardoor is de beoogde extra bescherming tenietgedaan. Voorstel is reeds voor uitlevering van ongeopende niet opgehaalde e-mail een extra bevel van de rechter-commissaris verplichten of het uitleveren van ongeopende en niet opgehaalde e-mail uit de uitleveringsplicht halen.

De regering heeft er voor gekozen het onderscheid tussen opgeslagen en stromende gegevens te handhaven, ondanks de kritiek die op dit voornemen is geuit door een aantal instanties. De leden van de GroenLinks-fractie kunnen daar gezien de aangevoerde argumenten mee instemmen, temeer nu een duidelijk onderscheiding de rechtszekerheid voor wat betreft de bijzondere opsporingsbevoegdheden ten goede komt.

6. Onderzoek van e-mail

De leden van de PvdA-fractie hebben zich reeds uitgelaten over de wenselijkheid van het maken van wetgeving op dit gebied, voorafgaand aan een ophanden zijnde grondwetswijziging. Zij vragen in hoeverre e-mail in de toekomst kan worden onderscheiden van andere vormen van content die providers aangeboden krijgen ter verwerking. Ziet de regering een dergelijk onderscheid? Zo ja, hoe zou zij dit omschrijven? Kan de regering op grond van het voorliggende wetsvoorstel nog eens de verschillen toelichten tussen bepalingen die betrekking hebben op e-mail in het bijzonder en die op content in het algemeen?
De leden van de PvdA-fractie hechten eraan dat genoemde gegevens slechts kunnen worden ingezien na tussenkomst van de rechter-commissaris. Daarmee is een redelijk evenwicht gevonden tussen enerzijds privacybelangen en anderzijds opsporingsbelangen.
Wel vragen deze leden de regering om duidelijk aan te geven welke maximumtijd mag verlopen tussen aanvraag van een verzoek om inzage bij de rechter-commissaris en mogelijke bewilliging in een dergelijk verzoek. De korpsbeheerders stellen in hun commentaar op het wetsvoorstel dat door te wachten op de tussenkomst van de rechter-commissaris er veel zaken stuk lopen. Kan de regering aard en aantal van deze volgens de korpsbeheerders stukgelopen zaken aangeven?

Bescherming van e-mail wordt meer van belang naarmate er meer van dit communicatiemiddel gebruik wordt gemaakt en er gevoeliger gegevens worden verstuurd. In dit verband hebben de leden van de VVD-fractie met belangstelling kennisgenomen van het rapport van de commissie Grondrechten in het digitale tijdperk. Ziet de regering naar aanleiding van de bevindingen van deze commissie aanleiding om de voorgestelde bescherming van e-mail aan te passen? Hoe beoordeelt zij in dit licht de aanbeveling dat enkel de aard van het gebruikte kanaal reeds als beslissend kan worden beschouwd voor de vraag of er sprake is van vertrouwelijke communicatie? Kan dit, in het geval van e-mail, betekenen dat alle e-mail berichten die niet worden verzonden naar een openbare list onder de (Grond)wettelijke bescherming vallen? De mogelijkheid tot vertrouwelijke communicatie is een belangrijk liberaal uitgangspunt. De leden van de VVD-fractie hechten daarom sterk aan een zeer duidelijke afbakening van e-mail berichten die wel en die niet onder de (Grond)wettelijke bescherming vallen. Belangrijk hierbij vinden zij dat persoonlijk geadresseerde e-mail zonder meer als vertrouwelijke e-mail moet worden aangemerkt. Deze leden vragen daarom wanneer moet worden aangenomen dat e-mail persoonlijk is geadresseerd. Is dit het geval indien het bericht wordt verstuurd aan een (grote) groep van mensen? Is dit het geval indien het bericht wordt verstuurd aan openbare mailgroepen? Is dit het geval indien het bericht wordt verstuurd aan mailgroepen die alleen toegankelijk zijn voor geregistreerde gebruikers?
De leden van de VVD-fractie vragen of het inderdaad zo is dat de geadresseerde achteraf kan constateren dat onbevoegd is kennisgenomen van zijn ongelezen e-mail. Is dit niet afhankelijk van de gehanteerde instellingen van het mailprogramma? En hoe beoordeeld de regering de mogelijkheid om via een internet mailprogramma pop-servers uit te lezen zonder dat hiervan via die pop-server melding van wordt gemaakt en zonder dat berichten automatisch in de map «gelezen» of iets dergelijks terechtkomen? Kan hier de vergelijking met de open gestoomde envelop worden gemaakt? Is mede op grond van deze mogelijkheden een ruimere strafrechtelijke bescherming van e-mail op zijn plaats?

De leden van de CDA-fractie vragen of in de praktijk voldoende duidelijk is wat onder e-mail verstaan moet worden. De memorie van toelichting spreekt van berichten die via computernetwerken worden verzonden. Dit

lijkt een erg ruim begrip. De raad van korpsbeheerders (politie) wijst erop dat de definitie zo ruim is dat bij een onderzoek in welke geautomatiseerde omgeving dan ook, er altijd vanuit moet worden gegaan dat er sprake zal zijn van gegevens die de status van e-mail zullen hebben. Voorstel is om voor alle duidelijkheid SMS berichten en soortgelijke communicatie gelijk te stellen aan e-mail. Ook andere dan internetnetwerken moeten steeds in ogenschouw te worden genomen. De memorie van toelichting heeft het over ISP's waar de discussie ook voor bijvoorbeeld mobiele telecomleveranciers van toepassing is.
In het wetsvoorstel wordt aangegeven dat slechts voor zover de afzender de van buitenaf kenbare wil heeft om het bericht vertrouwelijk te houden, e-mail een bijzondere strafrechtelijk bescherming verdient. De leden van de CDA-fractie vragen of de regering denkt dat in de praktijk altijd voldoende duidelijk zal zijn wanneer daarvan sprake is?
Het strafvorderlijk onderzoek van de e-mail wordt aan strenge voorwaarden gebonden. De leden van de CDA-fractie vragen waarom door de regering geen aansluiting is gezocht bij de artikelen 113 en 114 Sv, die gaan over inbeslagneming door de rechter-commissaris bij een gerechtelijk vooronderzoek.
Aan de strafvorderlijke kant gelden met betrekking tot e-mail de normale bepalingen betreffende het aftappen van telecommunicatie via openbare telecommunicatienetwerken. Het College van Procureurs-generaal heeft erop gewezen dat het niet gemakkelijk zal zijn het gegevensverkeer af te tappen. Berichten worden vaak in delen opgesplitst die langs verschillende wegen en technologische systemen naar het uiteindelijke doel worden geleid. Wat is de reactie van de regering hierop?

E-mail dient in het strafrecht in dezelfde mate beschermd te worden als een brief of een telefoongesprek, aldus de regering. Door de nieuwe technologie is het huidige artikel 13 Grondwet, waarin het brief-, telefoon- en telegramgeheim is opgenomen, gedateerd. Uiteindelijk moet e-mail hier ook onder gaan vallen. De regering wil echter niet wachten met de grondwetswijziging en stelt daarom nu reeds een aantal voorwaarden. E-mail wordt gedefinieerd als berichten die via computernetwerken worden verzonden. Is dit niet een wat al te ruim begrip, zo vragen de leden van de D66-fractie. Kan de regering het begrip wellicht nader preciseren?
De regering is van mening dat e-mail slechts een bijzondere strafrechtelijke bescherming moet verdienen voor zover de afzender de van buitenaf kenbare wil heeft om het bericht vertrouwelijk te houden. Zal in de praktijk altijd voldoende duidelijk zijn wanneer daarvan sprake is?
In de memorie van toelichting wordt de vraag opgeworpen of een Internet Service Provider zich schuldig maakt aan computervredebreuk als hij zonder toestemming van een abonnee in diens mailbox kijkt, omdat de mailbox zich namelijk bevind op een geautomatiseerd werk dat eigendom is van de provider. De regering stelt voor dat ISP's niet gerechtigd zijn kennis te nemen van niet voor hen bestemde gegevens die in hun computers zijn opgeslagen. In de praktijk is het echter zo dat niet af te leveren e-mail automatisch en in zijn geheel bij een functionaris, de op het Internet verplichte Postmaster, terechtkomt. Deze functionaris moet kennis nemen van de inhoud van de e-mail om te kunnen beoordelen of er technische fouten bestaan die gerepareerd kunnen worden en om te trachten de e-mail alsnog af te leveren. Kan de regering hier op reageren?

De bescherming van e-mail is onder de huidige wetgeving onvoldoende beschermd, zo menen de leden van de GroenLinks-fractie. Deze leden zijn van oordeel dat er zo spoedig mogelijk dient te worden voorzien in de (grond)wettelijke bescherming van e-mail, zoals die ook geldt voor brieven en telefoonverkeer. De Commissie «Grondrechten in het digitale tijdperk» heeft onlangs haar rapport aan de regering gezonden. In haar aanbevelingen gebruikt de Commissie alleen techniekonafhankelijke

formuleringen, zodat daar automatisch de bescherming van e-mail onder valt. In het licht van deze aanbevelingen zouden deze leden graag zien dat het onderhavige wetsvoorstel eveneens slechts techniekonafhankelijke formuleringen bevat. Gewezen wordt op de voorgestelde artikelen 273a tot en met 273d Sr. Deze leden zijn van mening dat met name genoemde artikelen zeer techniekafhankelijk zijn. Met relatief kleine aanpassingen kan naar de mening van deze leden in één artikel worden vervat waar nu vier artikelen voor nodig zijn. Het zou goed zijn reeds in dit stadium de aanbevelingen van de Commissie «Grondrechten in het digitale tijdperk» ter harte te nemen, temeer nu de regering in het onderhavige wetsvoorstel vooruit loopt op een eventuele grondwetswijziging.
Met de regering zijn de leden van de GroenLinks-fractie van oordeel dat ten aanzien van het transport van e-mail de bestaande wetgeving al in voldoende mate voldoet. De artikelen 139a tot en met 139c en artikel 374bis Sr (wordt 273d) zijn onverkort van toepassing op e-mail en aan het aftappen en opnemen van e-mail worden dezelfde eisen gesteld als aan het aftappen en opnemen van een traditioneel telefoongesprek (artikel 126m en 126t Sv).
Voor wat betreft opgeslagen gegevens zien de leden van deze fractie echter nog een punt van discussie. Is het zo dat de regering van oordeel is dat de bescherming van artikel 138a Sr zich niet uitstrekt tot bijvoorbeeld een medewerker van een bedrijf waar het gebruiken van een geheim password binnen het netwerk nagenoeg onmogelijk is? Zo ja, is dit niet in strijd met het recht op privacy van de betreffende medewerker? Het is deze medewerker immers niet vanzelfsprekend persoonlijk aan te rekenen dat hij persoonlijke gegevens aanwezig heeft in (een deel van) geautomatiseerde werken van een ander.

De leden van de SP-fractie vragen de regering toe te lichten in welk verband de mogelijkheid wordt geplaatst de e-mails te markeren als ongelezen. Indien een onbevoegde in een ongezien moment kennis neemt van de brievenbus van een derde, staat hem de mogelijkheid open na lezing deze te markeren als ongelezen. Voorts staat de persoon die op deze wijze wederrechtelijk kennis neemt van e-mail de mogelijkheid open de inhoud van de brief te kopiëren en weg te schrijven naar bijvoorbeeld een floppydisk. Kan de regering deze lezing bevestigen en daarmee vaststellen dat het dus wel degelijk mogelijk is informatie te vergaren zonder dat dit aan de rechtmatige eigenaar bekend hoeft te worden?
Is de regering met de leden van de SP-fractie van mening dat er richtlijnen of regelgeving zou moeten komen waarin het verplicht wordt gesteld om individuele computers in grote organisaties en netwerken beter te beveiligen dan thans het geval is? Te denken valt aan richtlijnen die computers hardwarematig of softwarematig verplicht beveiligen wanneer deze tijdens het werkproces niet in gebruik zijn. Dit kan niet alleen voor de betrouwbaarheid van het bedrijfsmatig functioneren van belang zijn, maar ook voor bijvoorbeeld privacygevoelige informatie zoals databestanden met persoonsgegevens. Hoe ziet de regering dit aspect – en risico – van het computergebruik?

Wat betreft de voorgestelde invulling van de lacune betreffende de bescherming van e-mail kunnen de leden van de SGP-fractie zich verenigen met de voorgestelde tekst van artikel 273d Sr. Zij hebben echter wel een vraag met betrekking tot de memorie van toelichting, waar voor de grondslag van de bescherming aansluiting lijkt te worden gezocht bij het geobjectiveerde wilscriterium dat ten grondslag lag aan het gesneuvelde voorstel tot wijziging van artikel 13 Grondwet (25 443). De vraag van deze leden is of de uitdrukkelijke keuze van de regering zich verdraagt met het inmiddels uitgebrachte advies van de Commissie Grondrechten in het digitale tijdperk.

7. Opsporingsonderzoek op openbare computernetwerken

In de memorie van toelichting wordt gesteld dat Nederlandse opsporingsambtenaren slechts onderzoek mogen doen op computernetwerken voor zover de Nederlandse rechtsmacht reikt. Hoe worden in dit verband computernetwerken van (mede) in Nederland gevestigde internationale organisaties of bedrijven beschouwd, vragen de leden van de PvdA-fractie. Voorziet het toekomstige verdrag van de Raad van Europa in deze en andere leemtes? Mogen op dit moment buitenlandse opsporingsambtenaren onderzoek doen in Nederlandse computernetwerken? Hoe wordt in dit verband het onderzoek gezien naar een strafbare inhoud op een stand-alone computer? Is het om opsporing te voorkomen of te hinderen slechts noodzakelijk dat dit apparaat de grens met België of Duitsland wordt overgebracht?

Openbare computernetwerken vormen een steeds grotere virtuele wereld. Net als in de echte wereld is ook in de virtuele wereld optreden van politie en justitie soms nodig. De leden van de VVD-fractie zijn beducht voor te grote inperking van de mogelijkheid voor politie en justitie om zich te bewegen op internet. Dit geldt versterkt voor die bewegingen die elke gewone burger wel is toegestaan te verrichten. Deze leden vragen om meer duidelijkheid over de grens tussen de bevoegdheden die een opsporingsambtenaar altijd mag uitoefenen en de bevoegdheden die slechts op grond van een speciale grondslag mogen worden uitgeoefend. Zo vragen zij wat zij in dit verband moeten verstaan onder stelselmatig onderzoek. Is hiervan spraken indien een bepaalde tijd op internet wordt doorgebracht, is het gebruik van een zoekmachine bepalend, gaat het om de mate van herhaling in het bezoek, de hoeveelheid gegevens die politie en justitie downloaden, de compleetheid van de gegevens die politie en justitie downloaden of gaat het om een combinatie van deze factoren? Moet onderzoek met behulp van «bots» worden aangemerkt als stelselmatig? Is dit ook het geval als de «bot» slechts één enkele keer bij een bepaald webadres op bezoek komt? Kan de regering aangeven in hoeverre zij dergelijke autonome, geautomatiseerde systemen toelaatbaar acht bij de opsporing en handhaving op internet?
Het voorliggende voorstel geeft onder andere enkele bepalingen over het hanteren van bijzondere opsporingsbevoegdheden op openbare netwerken. Uit een oogpunt van een effectieve opsporing is een mogelijkheid tot het hanteren van die bevoegdheden op een gesloten netwerk zoals een intranet waardevol. Hier staat tegenover dat de inbreuk op rechten van betrokkenen aannemelijker is. Zijn er naar de mening van de regering voldoende gronden om de bijzondere opsporingsbevoegdheden ook te hanteren op gesloten netwerken? Zo nee, waarom niet en zo ja, is de regelgeving, inclusief de hier voorgestelde wijzigingen, toegesneden op deze mogelijkheid?
De Nederlandse rechtsmacht strekt zich niet uit over computers in het buitenland, ook niet indien deze via een netwerk zijn verbonden met computers in Nederland. Wat echter de gewone burger mag, mag de opsporingsambtenaar ook, namelijk rondkijken op internet. Mag de opsporingsambtenaar, net als de gewone burger, ook gegevens downloaden van buitenlandse sites? De mogelijkheden tot het hanteren van opsporingsbevoegdheden op openbare netwerken wordt onder andere beperkt door de vraag of men redelijkerwijs kan vermoeden dat de gegevens zijn opgeslagen op een buitenlandse computer. Enerzijds begrijpen de leden van de VVD-fractie hieruit dat de beperking alleen van toepassing is op opgeslagen gegevens en niet op stromende gegevens. Anderzijds vragen zij zich af of bijvoorbeeld het adres in het netwerk voldoende aanwijzing vormt over de locatie van de computer. Mag bijvoorbeeld altijd een computer met een .nl adres worden doorzocht en bijvoorbeeld niet een .com-site? Wordt evenwel de opsporingshandeling abusievelijk toch

toegepast op een in het buitenland bevindende computer, dan moet onmiddellijk contact worden opgenomen met het buitenland. Welke gevolgen heeft dit voor de toelaatbaarheid van eventueel achterhaald bewijs? Kan er een herstel van het ontbreken van rechtsmacht plaatsvinden? Welke pogingen worden er ondernomen om het probleem van het ontbreken van internationale rechtsmacht op internet via een Verdrag op te lossen?
Over de pseudokoop merkt de regering op dat een burgerpseudokoop op internet niet wordt overwogen, omdat de tussenkomst van een netwerk het de politie mogelijk maakt om de pseudokoop altijd zelf uit te voeren. De leden van de VVD-fractie vragen of de politie dit inderdaad altijd zelf kan uitvoeren. Is het voorstelbaar dat een burgerinfiltrant gedurende zijn infiltratie gevraagd wordt van de zijde van de criminele organisatie om in hun fysieke aanwezigheid een koop via het internet te verrichten? Is het in dergelijke gevallen mogelijk dat de politie dit op afstand uitvoert? Doet het toenemend gebruik van internet de waarschijnlijkheid dat dergelijke situaties zich voordoen stijgen? Kan een toenemende vervlechting van de virtuele wereld met de echte wereld betekenen dat alsnog burgerpseudokoop via geautomatiseerde systemen wenselijk wordt?

Grootste obstakel in het wetsvoorstel is de reikwijdte van de Nederlandse rechtsmacht. Zo mag een opsporingsambtenaar volgens de memorie van toelichting geen bevoegdheden uitoefenen op sites die zijn opgeslagen in buitenlandse computers waarbij inbreuken op grondrechten worden gemaakt. De memorie van toelichting zegt dat indien een maatregel van ontoegankelijkmaking op goede gronden werd toegepast, maar later blijkt de maatregel de facto in een computer in het buitenland toegepast, er onmiddellijk contact moet worden opgenomen met de autoriteit van het desbetreffende land om te overleggen wat te doen. Dat wekt volgens het College van Procureurs-generaal de indruk alsof een vooraf niet bestaande bevoegdheid achteraf alsnog in het leven groepen kan worden. Volgens het College moet het van tweeën één zijn: of het is de opsporingsambtenaar niet toegestaan die bevoegdheden in het buitenland uit te oefenen, of het is hem wel toegestaan op basis van bestaande afspraken in het kader van wederzijds hulp. Kan de regering aangeven of er al verdragen in deze zijn of worden voorbereid?
Voor opsporingsambtenaren is het in het nieuwe wetsvoorstel niet nodig zich onder hun werkelijke naam bekend te maken. Alleen wanneer het onder pseudoniem opereren van een opsporingsambtenaar als misleiding van andere gebruikers van Internet moet worden aangemerkt, moet het hanteren van een pseudoniem ongeoorloofd worden geacht. De vraag kan worden gesteld of dit onderscheid wel altijd duidelijk te maken is.
Het zou wenselijk en ook strafvorderlijk mogelijk moet zijn om *interne* systemen met betrekking tot «stromende» gegevens aftapbaar of monitorbaar te maken. Op grond van artikel 125g Sv lijkt dat nu niet mogelijk. Voorstel is om in de redactie van artikel 125g de toevoeging «die wordt aangewend voor dienstverlening aan het publiek» geheel te laten vallen.
In artikel 139b lid 2 Sr wordt strafbaar gesteld het aftappen van gegevensoverdracht. Wat is de toegevoegde waarde van de term «heimelijk» naast de termen «opzettelijk en zonder daartoe gerechtigd te zijn»? Voorstel is met de woorden «opzettelijk en wederechtelijk» te volstaan.
De Tijdelijk Commissie Evaluatie Opsporingsmethoden is van mening dat pseudo-koop dient te worden opgevat als een vorm van infiltratie. De voor infiltratie geldende normen en procedures dienen volgens de commissie op een zelfde manier ook voor pseudo-koop te worden gevolgd. Vindt de regering dit ook?

De memorie van toelichting zegt dat indien bijvoorbeeld de maatregel van ontoegankelijkmaking op goede gronden werd toegepast, maar later blijkt dat, anders dan redelijkerwijs kon worden vermoed, de maatregel de facto

in een computer in het buitenland heeft plaatsgevonden, dan moet onmiddellijk contact worden opgenomen met de autoriteit van het desbetreffende land teneinde in onderling overleg te bezien wat er te doen staat. Dat wekt bij de leden van de fractie van D66 de indruk dat een niet vooraf bestaande bevoegdheid achteraf alsnog in het leven kan worden geroepen. Zou het niet zo moeten zijn dat het ofwel de opsporingsambtenaar niet is toegestaan die bevoegdheden in het buitenland uit te oefenen ofwel dat het hem wel is toegestaan maar dan op basis van reeds bestaande afspraken in het kader van de wederzijdse rechtshulp?
De leden van de fractie van D66 denken dat het wetsvoorstel slechts dan het beoogde effect zal sorteren wanneer er duidelijk internationale afspraken hierover zijn gemaakt, het internet is namelijk bij uitstek een geschikt middel om de nationale rechtsmacht te omzeilen. Wat is de mening van de regering op dit punt?
Gelet op het ingrijpende karakter van infiltratie is dit aan strikte voorwaarden verbonden. De memorie van toelichting vermeldt dat onder andere een bevel van de officier van justitie is vereist. Deze leden wijzen er op dat ook bij infiltratieacties in de digitale wereld toestemming van het College van Procureurs-generaal na advies van de CTC noodzakelijk is. Overigens is de Tijdelijke Commissie evaluatie opsporingsmethoden van mening dat pseudo-koop dient te worden opgevat als een vorm van infiltratie. De voor infiltratie geldende normen en procedures dienen ons inziens dan ook mutatis mutandis voor pseudo-koop te worden gevolgd. Kan de regering hierop reageren?

De leden van de GroenLinks-fractie betreuren het dat duidelijkheid met betrekking tot grensoverschrijdend opsporingsonderzoek ontbreekt, zolang het in voorbereiding zijnde verdrag betreffende de rechtsmachtskwesties er niet is. Het is deze leden voorts niet duidelijk of en hoe het eventueel mogelijk is onomstotelijk vast te stellen of een computer waarin een opsporingshandeling dient plaats te vinden zich *de facto* in het buitenland bevindt.
Uitbreiding van de artikelen 126i en 126q Sv zoals voorgesteld kan op instemming van deze leden rekenen. Zij blijven echter benadrukken dat de pseudokoop zoveel mogelijk dient te worden beperkt. Pseudokoop kan pas aan de orde zijn indien de inzet van dit middel strikt noodzakelijk is voor de opsporing en de verdachte mag op geen enkele wijze worden uitgelokt of aangezet tot het plegen van strafbare feiten. Aangenomen mag worden dat hierover duidelijke richtlijnen zullen worden aangereikt.

Ook bij dit onderdeel van het wetsvoorstel wordt de parallellen met wat verder is geregeld in de wet doorgetrokken, waarmee de leden van de fracties van RPF en GPV kunnen instemmen. Zij vragen evenwel of met name het zogeheten stelselmatig toepassen van opsporingshandelingen op internet in voldoende mate objectiveerbaar is te maken. Waar ligt precies die grens? In het bijzonder het stelselmatig downloaden van overigens openbare gegevens stelt deze leden voor vragen. Volgens de toelichting zouden deze gegevens niet mogen worden opgeslagen in een politieregister. Wordt de politie hiermee niet meer beperkt dan de burger, terwijl het uitgangspunt zou moeten zijn dat aan de politie in elk geval is toegestaan wat elke burger in de normale uitoefening van zijn burgerlijke vrijheden ook is toegestaan?
Verder vragen deze leden om een nadere toelichting op de praktische toepasbaarheid van het verbod om op buitenlandse netwerken opsporingshandelingen te verrichten. In hoeverre is duidelijk, of na te gaan of het buitenland zich op basis van wederkerigheid eveneens onthoudt van opsporingsonderzoeken in de Nederlandse virtuele ruimte? Hoe staat het met de internationale uitwisseling van gegevens, en de verschaffing aan buitenlandse opsporingsambtenaren om in elkaars virtuele ruimte onderzoek te verrichten? Hoe weet men of het om Neder-

landse of buitenlandse computernetwerken gaat, gezien de sterke onderlinge verwevenheid van netwerken? Hoe is een en ander toepasbaar bij stromende gegevens?
De leden van de fracties van de RPF en het GPV vragen om een nadere toelichting op het besluit om af te zien van het openen van de mogelijkheid van burgerpseudo-koop via een computernetwerk.
De leden van de fracties van de RPF en het GPV vragen om welke reden er wel een wijziging van de wet BOB nodig is voor digitale pseudokoop en niet voor digitale infiltratie.

De leden van de SGP-fractie hebben kennisgenomen van de voorstellen om gegevens ontoegankelijk te maken (artikel 125o Sv.). Dat ontoegankelijk maken zal naar hun opvatting in een zo vroeg mogelijk stadium moeten geschieden, dat wil zeggen al tijdens de huiszoeking en niet erna. De regering verwacht kennelijk dat die omslag zich automatisch zal voordoen. Deze leden vragen of dit niet een te optimistische vooronderstelling is, omdat voor onderzoek ter plekke heel wat technische ondersteuning en opleiding nodig is. Is daarin voorzien?
De uitbreiding van de mogelijkheid om gegevens af te nemen via een openbaar telecommunicatienetwerk beoordelen de leden van de SGP-fractie positief, evenals de uitbreiding van de waarborgen (opgave aan de beheerder en vernietiging van niet meer relevante gegevens) naar alle gevallen waarin gegevens worden aangetroffen in een geautomatiseerd werk. Zij stellen echter de vraag of de bescherming op één punt niet te ver doorschiet, namelijk waar opgave gedaan moet worden van vastlegging of ontoegankelijkmaking van gegevens aan de verdachte. Geldt dit ook voor de verdachte in een ander onderzoek (betreffende een andere verdachte)?
De leden van de SGP-fractie stellen de vraag of het uit wetsystematisch oogpunt wel zo wenselijk is om naast het onderscheid tussen opgeslagen en stromende gegevens, een onderscheid te maken tussen bestaande en toekomstige gegevens (zie artikel 125i Sv.). Ook plaatsen deze leden vraagtekens bij de doorverwijzing in bepalingen die ontsleuteling van telecommunicatie regelen. Zie 126 lid 6 Sv. – 126g lid 7 Sv. – 126g lid 1 Sv.
Tenslotte stellen de leden van de SGP-fractie de vraag hoe procedureel voortgegaan wordt met de behandeling van het onderhavige wetsvoorstel in relatie met de procedure betreffende het ontwerp verdrag van de Raad van Europa over computercriminaliteit.

8. Overige wijzigingen

De leden van de PvdA-fractie juichen de aanpak van spam en e-mailbombing van harte toe.

De belangrijkste overige wijziging die het voorstel met zich mee brengt is de strafbaarstelling van «bombing», stellen de leden van de VVD-fractie. Gekozen is voor een strafbedreiging van een jaar. Is e-bombing een ernstiger feit dan computervredebreuk? De keuze voor een strafbedreiging met een jaar brengt met zich mee dat de bevoegdheden van art. 16n en 126u Sv niet toepasbaar zijn bij een verdenking van e-bombing. Verdient het aanbeveling om de mogelijkheid tot het verkrijgen van inlichtingen over het gegevensverkeer dat via een openbare communicatienetwerk heeft plaatsgevonden, ook mogelijk te maken bij het delict «e-bombing»?
Er is voor gekozen om «spam» niet strafbaar te stellen. De grootschaligheid waarmee «spam» wordt uitgeoefend brengt evenwel een aanzienlijke economische schade met zich mee. Welke maatregelen acht de regering nodig om «spam» in te perken? Welke rol kan zelfregulering hierbij spelen? Wat is het standpunt van de regering met betrekking tot het voorstel van de Europese commissie om een database met daarin de mail-

adressen van mensen die geen «spam» wensen te ontvangen, zo vragen de leden van de VVD-fractie.
Gezien het sterk technische karakter van internet en de turbulente ontwikkelingen daarop, is de uitvoerbaarheid en handhaafbaarheid sterk afhankelijk van de inzet die politie en justitie op dit terrein kan maken. Ontwikkeling van speciale expertise is noodzakelijk. Hiertoe dienen mede de bureaus digitale expertise. Kan de regering een nadere toelichting geven op het functioneren van deze bureaus? Zoals toegezegd zal er nog een standpunt volgen van de regering over de aanvullende eisen met betrekking tot uitrusting, organisatie en opleiding van politie en justitie. De regering geeft echter niet aan welke rol zij ziet weggelegd voor zelfregulering en meldpunten. De leden van de VVD-fractie vragen de regering om alsnog hierop in te gaan.
In de Wet bescherming persoonsgegevens zijn ook bepalingen opgesteld met betrekking tot het ontvangen van ongewenste post of e-mail. Kan de regering daarover een uiteenzetting geven en daarbij aandacht besteden aan een mogelijke leemte tussen beide wetten?

De leden van de D66-fractie stellen dat spam (het ongevraagd toezenden van grote hoeveelheden e-mail) op Internet in toenemende mate als een probleem wordt ervaren. Valt spam nu onder de strafbepaling van artikel 138b Sr? Zo nee, waarom ziet de regering geen rol voor het strafrecht weggelegd als het gaat om tot een verbod op spam te komen? Spam geschiedt namelijk, net als bij ongevraagde commerciële faxen die wel verboden zijn, op kosten van onder andere de ontvanger. Bovendien bestaat de kans dat de apparatuur van de ontvanger onbruikbaar wordt en is spam door iedereen ongewenst. Er is dus ook nog eens sprake van een inbreuk op de privacy. Kan de regering ingaan op de vraag waarom er geen algemeen verbod van spam is opgenomen in het onderhavige wetsvoorstel?

Zoals hiervoor al beargumenteerd, wordt het door de leden van de GroenLinks-fractie betreurd dat de regering bij het voorstel de artikelen 372 tot en met 375 Sr over te hevelen naar titel XVII van boek 2 betreffende «schendingen van geheimen» niet van de gelegenheid gebruik heeft gemaakt een techniekonafhankelijke terminologie te gebruiken. De regering noemt als argument hiervoor onder meer dat Nederland op grond van het ITU verplicht is telegrafie als dienst in stand te houden. Dit staat echter los van de mogelijkheid de strafbaarstelling van schendingen van geheimen door een bepaalde groep personen techniekonafhankelijk te omschrijven. Hier zou de telegrafie immers ook onder blijven vallen, menen deze leden. Is de regering bereid genoemde artikelen in die zin te wijzigen, zodat ook al wordt voldaan aan de aanbevelingen van de Commissie «Grondrechten in het digitale tijdperk».
Met de wijziging van de artikelen 350a en 350b Sr en het opnemen van artikel 138b Sr kunnen deze leden instemmen. De hiermee te beschermen belangen zullen een steeds grotere plaats innemen in de mogelijkheden voor een ieder om ongehinderd gebruik te kunnen maken van een gekozen communicatiemiddel. De leden van de GroenLinks-fractie vragen wel of nader gespecificeerd zou kunnen worden wanneer sprake is van «bestemd om diens toegang tot dat netwerk of die dienst te belemmeren». Dat hierover meer duidelijkheid komt is van belang nu niet vereist is dat door de gedraging de toegang tot het netwerk of de dienst daadwerkelijk wordt belemmerd.

Naar aanleiding van de nieuwe strafbepaling over «e-mail bombing» (art. 138b Sr.) stellen de leden van de SGP-fractie de vraag of zij het juist zien dat de bepaling niet van toepassing is op wat wel (klassieke) spam wordt genoemd, te weten het ongevraagd toesturen van e-mail aan een groot aantal personen, wat meestal gebeurt in het kader van direct marketing. Is

het in dit licht beschouwd wel zo gelukkig dat de memorie van toelichting voor het verstoppen van iemands e-mailbus de term «spam» gebruikt? Ook hebben deze leden bij deze bepaling de vraag of de maximaal mogelijke gevangenisstraf (een jaar) wel zo gelukkig is gekozen, aangezien de meest voor de hand liggende opsporingsbevoegdheid, namelijk die van de artikelen 126u en 126v, niet toegepast kan worden. Zou het daarom geen overweging verdienen om – evenals bij computervredebreuk is gebeurd – in de artikelen 126u en 126v Sr. expliciet te vermelden dat deze bevoegdheid ook ter opsporing van het feit van artikel 138b Sr. kan worden toegepast?

9. Handhaving

Zoals eerder aangehaald is de rechtsmacht in dit voorstel een groot probleem. Heeft de regering ook overwogen de in het buitenland gepleegde strafbare feiten door uitbreiding van artikel 4 Sr onder het bereik van de Nederlandse rechtsmacht te brengen, zoals gesuggereerd door het College van Procureurs-generaal vragen de leden van de CDA-fractie.
Uit het actieprogramma «Op weg met digitaal rechercheren», dat door de politie zelf is voortgebracht is gebleken dat de ontwikkeling van digitaal rechercheren onvoldoende is. Het gaat te langzaam en er is nog geen sprake van een landelijk dekkend netwerk. Het wetsvoorstel zelf leidt niet tot aanvullende eisen met betrekking tot de organisatie, uitrusting of opleiding van politie of justitie. Kan de regering een toelichting geven op het functioneren van de huidige interregionale bureaus digitale expertise? Denkt de regering dat een uitbreiding van de recherche capaciteit nodig is?
Kan de regering tenslotte aangeven of de wet Computercriminaliteit I concreet en in de praktijk veel gebruikt wordt?

Zoals reeds eerder vermeld acht de D66-fractie een goede samenwerking tussen opsporingsdiensten een vereiste, teneinde een effectieve rechtshandhaving te kunnen waarborgen. Hoe staat het met de samenwerking tussen de autoriteiten van de verschillende landen van europa voor wat betreft de opsporing. Worden afspraken gemaakt binnen de Raad van Europa?
Opslag van gegevens in het buitenland is met behulp van internet gemakkelijker geworden. Kan een Nederlandse provider eventuele strafrechtelijke aansprakelijkheid ontlopen door de informatie op een buitenlands computersysteem te plaatsen? Heeft de regering ook overwogen de in het buitenland gepleegde strafbare feiten door uitbreiding van artikel 4 Sr onder het bereik van de Nederlandse rechtsmacht te brengen, zo vragen de leden van de D66-fractie.

De leden van de GroenLinks-fractie hebben ernstige twijfels over de deskundigheid en capaciteit binnen het politieapparaat, het openbaar ministerie en de rechtbanken. De regering stelt dat de regionale politiekorpsen inmiddels beschikken over zeven Interregionale bureaus digitale expertise die waar nodig bij opsporingsonderzoeken ondersteuning verlenen, maar is het niet zo dat deze bureaus reeds onder de huidige wetgeving de hulpvragen niet aankunnen? En is er bij binnen OM en rechtbanken sprake van educatie die kennis van de technische ontwikkelingen enigszins waarborgen? Zo ja, hoe ziet die educatie eruit? Zo nee, hoe denkt de regering deze achterstand in te halen?

De leden van de fracties van de RPF en het GPV vragen om meer informatie over de capaciteit van de opsporingsdiensten om ter zake van de computercriminaliteit effectief op te treden. Er wordt wel gesproken over kennis, maar nauwelijks over capaciteitsuitbreiding. Hoe staat het met de

huidige beschikbare capaciteit voor deze gespecialiseerde vorm van opsporing Is de politie in staat de benodigde kennis te verwerven?

De leden van de SGP-fractie kunnen zich verenigen met het voornemen om de bevoegdheid iemand te bevelen te ontsleutelen uit te breiden. Zij vragen of de vervanging van de terminologie «bij» de doorzoeking door «bij of terstond na» de doorzoeking ver genoeg gaat. Zij denken daarbij aan inbeslagneming van een schootcomputer bij aanhouding, staande houden of heterdaad (artikelen 95–96), of door de rechter-commissaris tijdens een gerechtelijk vooronderzoek (art. 104 Sv.). Evenmin als bij een bevel tot toegangsverschaffing (art. 125k lid 1 Sv.) – dat ook beperkt is tot doorzoeking –, bevreemdt het deze leden dat het wetsvoorstel deze bevelen niet uitbreidt tot alle gevallen van onderzoek in een geautomatiseerd werk.
Wat betreft de uitbreiding van artikelen betreffende de telefoontap (artikelen 126m en 126t Sv.) stellen deze leden de vraag of het feit dat eventuele ontsleuteling pas plaats kan vinden nadat het tappen is afgelopen complicaties oplevert voor de eis dat het bevel «bij of terstond na» de uitoefening van de tap moet worden gegeven, zeker wanneer de tap vele maanden lang duurt.
Ook vragen deze leden hoe werkbaar deze bepaling is, gegeven de omstandigheid dat bij versleutelde telefoongesprekken en faxen de sessiesleutel direct na afloop wordt weggegooid en de wet geen verplichting bevat om de sleutel te bewaren.
Ook vragen deze leden hoe de bewijskracht van de oorspronkelijke communicatie komt vast te staan en is gewaarborgd, gelet op de voorgeschreven wijze van medewerking aan ontsleuteling. Zal de ontsleuteling in de rechtszaal herhaald moeten worden? Hoe verhoudt zich dit tot de eis dat het bevel tot ontsleuteling niet tot de verdachte mag worden gericht?
Tenslotte stellen deze leden de vraag of, gegeven het feit dat het om een soortgelijk bevel gaat, het bevel tot ontsleuteling bij gegevensopslag (artikel 125k lid 1) en het bevel tot ontsleuteling bij telecommunicatie (artikelen 136m lid 5 en 126t lid5) in identieke bewoordingen zouden dienen te worden vervat.

ARTIKELSGEWIJS DEEL

Artikel I

C

Kan de regering door middel van voorbeelden nader verduidelijken wat onder een geautomatiseerd werk dient te worden verstaan, vragen de leden van de D66-fractie.

K

De strafbepaling over het vervalsen van betaalpassen en waardekaarten wordt in het voorstel verduidelijkt en uitgebreid, doordat de bepaling ook van toepassing wordt op kaarten als telefoonkaarten en kopieerkaarten. In de memorie van toelichting wordt de bescherming van waardekaarten beperkt tot die kaarten die voor het publiek beschikbaar zijn, zulks vanwege het in geding zijnde maatschappelijke vertrouwen. Om die reden worden kaarten die voor gebruik in besloten kring bedoeld zijn uitgesloten. De vraag van de leden van de SGP-fractie is of deze redenering wel steeds opgaat, bijvoorbeeld wanneer een toegangspas voor werknemers

van een bepaald bedrijf tevens betaalmogelijkheden in zich bergt. Kan ook dan het maatschappelijk vertrouwen niet in geding komen? Zij vragen daarom of de zinsnede «voor het publiek beschikbare» geen heroverweging verdient.

De voorzitter van de vaste commissie voor Justitie,
Van Heemst

De griffier voor dit verslag,
Fenijn