Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1997–1998

25 443 Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepalingen inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim

Nr. 5

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 18 november 1997

1. Algemeen

1.1. Betekenis en reikwijdte van het nieuwe artikel 13

Met belangstelling hebben wij kennis genomen van de reactie van de leden op het verklaringsvoorstel, waarbij het briefgeheim en het telefoon- en telegraafgeheim worden uitgebreid tot een algemeen recht op vertrouwelijke communicatie. Wij hopen met deze nota er aan te kunnen bijdragen dat de plenaire behandeling van het voorstel in de Tweede Kamer voor het eind van het jaar plaatsvindt. In dat geval bestaat er een goede kans de eerste lezing nog in deze kabinetsperiode te voltooien.

De leden van de PvdA-fractie meenden dat het nu geldende briefgeheim met het voorstel wordt ontkracht en spraken over een verwarrende formulering van de reikwijdte van het grondrecht in de memorie van toelichting. Naar de mening van de leden van de CDA-fractie leidt het regeringsvoorstel tot een geringere bescherming van de bestaande communicatiemiddelen dan de huidige bepaling biedt. De leden van de D66-fractie waren het eens met de achterliggende gedachte van het voorstel, maar zij hadden twijfels over de uitwerking. Zij meenden dat het voorstel vele vormen van communicatie vogelvrij maakt. De leden van de fracties van de RPF en de SGP hadden enkele vragen naar aanleiding van reacties op het voorstel in de literatuur; ook andere fracties verwezen naar de literatuur. De leden van de GPV-fractie meenden dat niet een goede afweging is gemaakt tussen het recht op vertrouwelijke communicatie en de noodzaak van beperking van dat recht.
Hoewel wij deze kritiek niet delen, begrijpen wij de kritische toon wel. De memorie van toelichting geeft, bij nader inzien, niet voldoende duidelijk onze gedachtegang weer. Ook de antwoorden op vragen van de leden Van Zuijlen en Roethof[1] – in het verslag wordt verschillende keren naar deze antwoorden verwezen – kunnen aan deze onduidelijkheid hebben bijgedragen. Wij willen in het navolgende proberen meer duidelijkheid te geven, om aldus de aarzelingen die bij vele leden zijn ontstaan te kunnen wegnemen.
Met de nieuwe tekst van artikel 13 wordt niet beoogd de nu in het artikel neergelegde rechten te beperken. Bedoeld is om, naast het briefgeheim

[1] Tweede Kamer, vergaderjaar 1996/97, aanhangsel 1370.

KST25589
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 1997

en het post- en telegraafgeheim, ook andere vormen van vertrouwelijke communicatie grondrechtelijk te beschermen. De wijziging van artikel 13 betekent dat het bestaande beschermingsniveau wordt uitgebreid tot de nieuwe communicatietechnieken die, naast post, telefonie en telegrafie, zijn ontstaan, zonder aan de bestaande bescherming enige afbreuk te doen, en dat de grondwettelijke bescherming eveneens ten deel zal vallen aan communicatietechnieken die in de toekomst tot ontwikkeling komen. Om dit mogelijk te maken is gekozen voor de techniek-onafhankelijke benadering die besloten ligt in het begrip «vertrouwelijke communicatie».
Voor een goed begrip van de reikwijdte van het grondrecht op vertrouwelijke communicatie is het van belang om de verschillende fasen die zich bij communicatie (kunnen) voordoen te onderscheiden. De te onderscheiden fasen zijn:

– de aanmaak- en verzendfase
– de transportfase
– de ontvangstfase
– de tussentijdse opslag tijdens het transport
– de opslag bij de verzender of de ontvanger.

Opslag doet zich niet voor bij elke vorm van communicatie, maar komt wel steeds meer voor. De klassieke vorm van opslag is de postbus op het postkantoor. Een modernere vorm is de E-mailbox bij de provider. Het over de telefoon gesproken woord kan worden opgeslagen bij de ontvanger (antwoordapparaat) of bij de transporteur (voice-mail).
Tegenwoordig is vaak in technische zin sprake van opslag (in een digitale omgeving gaat transport altijd gepaard met opslag, hoe kort die opslag ook is), terwijl dat juridisch niet relevant hoeft te zijn. Van opslag in juridische zin is sprake wanneer gegevens kunnen worden geraadpleegd op een door de mens te bepalen tijdstip; er is daarentegen sprake van transport wanneer gegevens zich bevinden in een toestand van telecommunicatie.
De vraag of sprake is van bescherming door artikel 13 is afhankelijk van het communicatiemiddel en in bepaalde gevallen ook van de fase waarin men zich bevindt. Artikel 13 strekt ertoe om alleen communicatie te beschermen die vertrouwelijk is. De vertrouwelijkheid moet blijken uit de geobjectiveerde wil van de verzender om de communicatie vertrouwelijk te houden. De geobjectiveerde wil is aanwezig wanneer een derde een bepaalde hindernis moet nemen om van de informatie kennis te nemen. Die hindernis hoeft niet heel groot te zijn, voldoende is dat uit de hindernis blijkt dat de wil van de verzender gericht is op vertrouwelijkheid. Van een hindernis is sprake wanneer een E-mailbericht is beveiligd door encryptie of eenvoudiger door een password. Ook het eenvoudig dichtplakken van een envelop is vanzelfsprekend een hindernis die voldoende is om de bescherming van artikel 13 te kunnen aannemen.
Het grondwettelijke briefgeheim ondergaat door de voorgestelde wijziging van artikel 13 qua reikwijdte geen wijziging. Het briefgeheim geldt vanaf het moment dat de verzender de brief heeft dichtgeplakt, het geldt met name voor de transportfase, maar het briefgeheim geldt ook wanneer de ontvanger de brief nog niet heeft geopend. Wanneer de ontvanger de brief in zijn woning geopend op tafel neerlegt, geldt het briefgeheim niet meer. Wel wordt de brief dan onder omstandigheden beschermd door artikel 10, eerste lid (eerbiediging van de persoonlijke levenssfeer) en indirect door artikel 12 (onschendbaarheid van de woning).
Artikel 13 strekt dus ertoe om vertrouwelijke communicatie te beschermen. In sommige gevallen is de werking echter ruimer en komt grondwettelijke bescherming toe aan een communicatie*medium,* ook al is niet al het transport dat via dat medium loopt vertrouwelijke communicatie. Er zijn naar de huidige stand twee gevallen van bescherming op het niveau van het communicatiemedium.
1°. Artikel 13 beschermt alle telecommunicatie die plaatsvindt over het vaste openbare telefoonnet. De reden voor deze radicale bescherming is

gelegen in de technische kenmerken van het telefoonnet. Het is niet mogelijk de verschillende soorten van communicatie te onderscheiden zonder eerst kennis te nemen van de inhoud van communicatie. Pas bij het aftappen van een gegevensstroom kan blijken of sprake is van een vertrouwelijk telefoongesprek. De enige manier om de vertrouwelijke communicatie over telefoonlijnen te beschermen, is door alle verkeer over het vaste openbare telefoonnet te beschermen.
Het hier gestelde geldt overigens ook voor de digitale openbare telefoonnetwerken van, bijvoorbeeld, PTT Telecom en Libertel. Een uitzondering geldt alleen voor analoge mobiele telefoonnetten die op eenvoudige wijze zijn af te luisteren, zoals ATF 3. Bij de grondwetsherziening 1983 gold dit uitgangspunt ook al.[1]
Als gevolg hiervan wordt niet alleen het gewone kabelgebonden en digitaal mobiele telefoonverkeer beschermd, maar ook alle E-mail- en faxverkeer gedurende het transport over het telefoonnet. Feitelijk is dus ook een telefoongesprek waarmee rechtstreeks in een radio-uitzending wordt meegepraat beschermd tegen het aftappen van de telefoonlijn, hoewel het evident is dat de beller geen behoefte heeft aan vertrouwelijkheid. De bescherming is dan beperkt tot de transportfase over de telefoonlijn. Ook beschermd is het transport van gegevens van en naar een Internetpagina, die ter beschikking wordt gesteld aan alle gebruikers van Internet. Ook daar ontbreekt het vertrouwelijke karakter, maar is er toch bescherming. Tenslotte, wanneer iemand vanaf een Internetpagina een computerprogramma naar zijn eigen computer binnenhaalt *(downloadt),* zou twijfel kunnen bestaan over de vraag of er sprake is van communicatie. Wat daarvan zij, ook dit wordt beschermd, omdat het over een telefoonlijn plaatsvindt.
2°. Artikel 13 beschermt om dezelfde reden alle enveloppen die zijn dichtgeplakt en aan de post worden toevertrouwd. Een envelop bevat in sommige gevallen een brief die niet vertrouwelijk hoeft te blijven (bijvoorbeeld: een pamflet). Ook kan het zijn dat de inhoud van de envelop geen communicatie is (vakantiefoto's zonder begeleidend briefje). Toch geldt in al deze gevallen het aloude briefgeheim. De postbezorger zou immers eerst kennis moeten nemen van de inhoud om te kunnen vaststellen of sprake is van vertrouwelijke communicatie.
Deze bescherming van het communicatiemedium sluit overigens aan bij een opmerking van de leden van de VVD-fractie, die, bij de bespreking van het eerste lid in het verslag, hebben gepleit voor de vertrouwelijkheid van het communicatiekanaal.

1.2. Faxverkeer

Veel leden hebben vragen gesteld over de status van faxberichten. De strekking van deze vragen is steeds, dat de fax onder de bescherming van artikel 13 dient te vallen.
Op bladzijde 2 van de memorie van toelichting is opgemerkt dat bij gewone faxen niet op geheimhouding mag worden gerekend. Met deze passage werd gedoeld op de geheimhouding van het faxbericht dat bij de ontvanger in de vergaarbak is beland, niet op het faxverkeer over de telefoonlijn.
Faxberichten, zo merken wij op, zijn tijdens het transport over het telefoonnet beschermd door artikel 13. Deze bescherming vloeit voort uit het feit dat, zoals hiervoor opgemerkt, alle dataverkeer over het telefoonnet is beschermd. Faxberichten zijn dus tijdens de verzending evenzeer beschermd als telefoongesprekken. Bij de ontvangst van faxberichten ligt dit anders. Afgezien van het zeer zeldzame geval van sealfax[2] is een faxbericht dat uit het faxapparaat rolt, in principe toegankelijk voor iedereen die toegang heeft tot de ruimte waarin het faxapparaat staat opgesteld. Wie een faxbericht verstuurt zal er doorgaans rekening mee moeten houden dat zijn bericht aan de kant van de

[1] Kamerstukken 13 872, nr. 3, blz. 46.
[2] Een sealfaxbericht wordt, zodra het uit het faxapparaat rolt, verzegeld. Sealfax is dus, bij de ontvangst, grondrechtelijk op één lijn te stellen met een gesloten brief.

ontvanger niet strikt vertrouwelijk is, met name wanneer (zoals meestal) het faxapparaat op een kantoor staat opgesteld. Door te kiezen voor het middel van de fax aanvaardt hij dit gegeven.
De conclusie is dat faxberichten tijdens de verzending wel worden beschermd door het grondrecht op vertrouwelijke communicatie, maar niet meer na de ontvangst.

1.3. E-mail

De vragen over elektronische post (E-mail) staan deels in het algemeen gedeelte van het verslag, deels bij de bespreking van het eerste lid. Voor de overzichtelijkheid worden ze op deze plaats behandeld.
Op bladzijde 2 van de memorie van toelichting hebben wij aangegeven dat beveiligde computerberichten over het datanetwerk beschermd worden. Hieronder moeten ook begrepen worden berichten die met een wachtwoord (password) zijn beveiligd. Immers, alvorens derden kennis kunnen nemen van de communicatie-inhoud zullen zij een hindernis moeten nemen, bestaande uit het kraken van het password.
Voor de helderheid willen wij graag enkele begrippen afbakenen. In het gewone spraakgebruik wordt onder E-mail meestal verstaan: elektronische berichten die alleen gericht zijn aan en bestemd zijn voor één of enkele geadresseerden. Op zichzelf is echter ook sprake van E-mail wanneer iemand een bericht in een nieuwsgroep op Internet of op een bulletin board (BBS) plaatst; zo'n bericht is algemeen toegankelijk en de verzender wil ook dat het bericht openbaar is. Dergelijke E-mailberichten vallen niet onder het begrip «vertrouwelijke communicatie».
Het geheel overziend menen wij dat E-mail in vrijwel alle gevallen wordt beschermd door artikel 13. Daarvoor zijn er twee redenen.
1.° E-mail wordt zonder meer beschermd tijdens de fase van het transport over het telefoonnet. Immers, het telefoonnet als zodanig is beschermd, een bescherming die zich uitstrekt tot alle vormen van dataverkeer die over het telefoonnet lopen.
2.° Voor zover het gaat om de andere fasen van het E-mailverkeer (opslag bij de verzender, de ontvanger of de provider) is het technische karakter van E-mail bepalend. E-mail is praktisch gesproken altijd beschermd door middel van een password, dat alleen aan de gebruiker bekend is. Wie een E-mailbericht wil ophalen bij de provider moet zich namelijk identificeren door het opgeven van een password.[1] Artikel 13 verlangt dat de geobjectiveerde wil om de communicatie vertrouwelijk te houden blijkt uit een bepaalde hindernis, die een derde moet nemen om van de communicatie kennis te kunnen nemen. Als hindernis is het password voldoende.
Een E-mailbericht kan verdergaand beveiligd worden door codering van het bericht (versleuteling of encryptie). Dat leidt tot een verdergaande feitelijke bescherming omdat *hacken* moeilijker wordt, maar het is niet noodzakelijk voor de juridische bescherming die artikel 13 verleent. Dat het password eventueel gekraakt kan worden doet aan die juridische bescherming niet af. Ook een dichtgeplakte brief is eenvoudig open te scheuren of open te stomen, terwijl dan toch sprake is van schending van het briefgeheim. Als iemand een persoonlijk gericht E-mailbericht dat niet voor hem bestemd is, zonder toestemming van de ontvanger ophaalt bij de provider, is er sprake van computervredebreuk (artikel 138a Wetboek van Strafrecht). Hij kan dit bijvoorbeeld doen door het opgeven van een password dat hij niet mag kennen. Dan is sprake van het aannemen van een valse hoedanigheid in de zin van artikel 138a.
Een E-mailbericht is alleen dan niet beschermd wanneer de verzender zelf door handelingen te kennen geeft geen aanspraak op bescherming te willen maken. Dit doet zich voor wanneer hij een E-mailbericht adresseert aan een nieuwsgroep op Internet (zij het dat het transport van het bericht over het telefoonnet wel beschermd is) of wanneer hij het anderszins openbaar maakt. De bescherming van artikel 13 vervalt ook wanneer een

[1] Het password kan eventueel worden gegenereerd door de PC van de ontvanger. De ontvanger merkt dan niet dat het password wordt ingevuld en kan zelfs in de veronderstelling verkeren dat hij zonder password werkt. Dit technische aspect maakt voor ons betoog geen verschil.

verzonden of nog te verzenden bericht op de computer van de verzender staat en het bericht niet door een wachtwoord of anderszins is beveiligd. Het bericht is dan te vergelijken met een tekstdocument dat op de computer wordt bewaard, of een brief die – uit de envelop – onbeschermd op tafel ligt. Uiteraard zal er onder omstandigheden wel bescherming zijn door artikel 10 (persoonlijke levenssfeer) en – voorzover de computer in een woning staat – in beginsel door artikel 12 (onschendbaarheid van de woning).
Het is overigens goed om te bedenken dat de hiervoor (paragraaf 1.1) al genoemde vragen van de leden Van Zuijlen en Roethof aan de Minister van Justitie betrekking hadden op een vrij specifiek geval. Het ging om een E-mailbericht dat via Internet openbaar was gemaakt; het openbaar ministerie had alleen de identiteit van de verzender opgevraagd bij twee Internetproviders. Het spreekt vanzelf dat een E-mailbericht dat door de verzender openbaar is gemaakt niet onder het begrip «vertrouwelijke communicatie» valt. Waar in het antwoord op vraag 6 wordt gesproken over het briefgeheim, ging het niet om het grondwettelijke begrip, maar om het begrip zoals dat in het strafrecht is uitgewerkt. Dit begrip heeft een beperkter reikwijdte dan het grondwettelijke begrip.
De leden van de fractie van de PvdA hebben vragen gesteld over de bevoegdheid van Internet-providers om de mailboxen van gebruikers te openen. Binnen de brancheorganisatie van Nederlandse Internetproviders (de NLIP) wordt gewerkt aan algemene voorwaarden, waarin onder meer zal worden geregeld dat providers geen mailboxen mogen inzien.[1]
Hoewel deze vorm van zelfregulering een positieve ontwikkeling is, zijn wij voornemens het kennisnemen van deze mailboxen strafbaar te stellen. Het kennisnemen zal, analoog aan het tapverbod in artikel 139c Wetboek van Strafrecht, alleen zijn toegestaan:
– indien dit dient ten behoeve van de strafvordering,
– als het plaatsvindt in het kader van de taakuitoefening door een inlichtingen- of veiligheidsdienst, op bijzondere last van de verantwoordelijke minister of ministers, of
– als het kennis nemen noodzakelijk is om technische redenen (onderhoud, controle).

Wij menen dat de stelling, dat E-mail- en faxverkeer met het nieuwe artikel 13 vogelvrij zouden worden, hiermee voldoende is weersproken.

1.4. Beeld

In de memorie van toelichting is gesteld dat onder het begrip communicatie uitsluitend geschreven en auditieve communicatie moeten worden verstaan, zodat beelden hier niet onder vallen. Deze passage heeft aanleiding gegeven voor vragen. De leden van de PvdA-fractie hebben geïnformeerd of een foto die per brief of per E-mail wordt verstuurd, niet beschermd is. Zij wezen erop dat steeds meer convergentie optreedt tussen beeld, geluid en tekst. Zij noemden beeldtelefoon en videoconferencing als voorbeelden. De leden van de fracties van het CDA, de VVD, D66, de SGP en het GPV hebben soortgelijke vragen gesteld.
Graag merken wij het volgende op. Artikel 13 strekt primair tot bescherming van vertrouwelijke communicatie. Een tekst is op zichzelf geen communicatie (en dus niet beschermd door artikel 13), maar zij wordt dat wel zodra de tekst wordt verstuurd. Uit de keus voor een communicatiemiddel (zoals brief of E-mail) mag worden afgeleid dat communicatie is beoogd. Hetzelfde geldt voor een foto of een ander beeld. Wat in de toelichting werd beoogd te zeggen is, dat een beeld niet vaak voor directe communicatie wordt gebruikt, zodat de bescherming van artikel 13 minder snel aan de orde is. Dat neemt niet weg dat, wanneer iemand een foto zonder begeleidende brief in een gesloten envelop verstuurt, de verzending zonder meer wordt beschermd door het briefgeheim. Of de foto naar zijn inhoud een communicatieve functie heeft is in die situatie niet van belang.

[1] Informatie hierover is te vinden op de Internetpagina van de NLIP. Het adres is http://www.nlip.nl.

Het verschil tussen tekst en geluid enerzijds en beeld anderzijds speelt wel een rol bij een gesprek dat vertrouwelijk wordt gevoerd. In de toelichting werd al aangegeven dat een deelnemer aan een gesprek in een café er rekening mee moet houden dat anderen die vlakbij zitten het gesprek kunnen volgen. Hij hoeft echter geen rekening te houden met afluisteren door middel van technische apparatuur. Artikel 13 is dan in het geding. Wordt echter een video-opname zonder geluid van het gesprek gemaakt, dan zal in het algemeen artikel 13 niet in geding zijn: de communicatie tussen de deelnemers is meestal niet met een video-opname vast te leggen. Dit wordt anders wanneer het mogelijk wordt om het gesprek met behulp van de videoband te volgen door middel van lipleestechnieken. Overigens is het heimelijk maken van video-opnames doorgaans wel een schending van artikel 10.
Wordt beeld gecombineerd met geluid, zoals bij beeldtelefoon of videoconferencing, dan is in ieder geval sprake van communicatie via geluid. Het zou kunstmatig aandoen om beeld en geluid te scheiden. De beelden zijn dan tijdens de transportfase beschermd, omdat zij via het telefoonnet worden doorgegeven. Of de beelden zoals die bij de deelnemers aan het gesprek op een beeldscherm verschijnen, ook worden beschermd, hangt van de bedoeling van de deelnemers af. Een beeldscherm is moeilijker af te schermen dan de hoorn van een telefoon. De deelnemers zullen dus iets minder snel aanspraak kunnen maken op strikte vertrouwelijkheid. Staat echter de bedoeling voorop een strikt besloten gesprek of vergadering te houden, dan mogen de deelnemers van elkaar verwachten dat zij passende maatregelen treffen, bijvoorbeeld: dat zij de deur op slot doen.
Foto's, tekeningen of andere afbeeldingen die per gesloten envelop worden vervoerd, vallen zonder meer onder de bescherming van artikel 13. Hiervoor werd immers al opgemerkt dat de gesloten envelop die per post wordt vervoerd, ongeacht de inhoud, altijd onder artikel 13 valt. Hetzelfde geldt voor digitale beelden die via Internet of E-mail worden vervoerd: voor de duur van het vervoer vallen deze onder de algemene bescherming van het telefoonnet. Dat betekent dat de vraag of beeld onder het begrip «communicatie» gerekend moet worden vooral theoretische betekenis heeft.

1.5. Mondelinge gesprekken

De leden van de CDA-fractie hebben opgemerkt dat de bescherming van het vertrouwelijke gesprek wordt overgebracht van artikel 10 Grondwet naar artikel 13. Hun is niet gebleken dat artikel 10 onvoldoende waarborg biedt.
Anders dan de genoemde leden achten wij het van groot belang dat juist ook het vertrouwelijke gesprek onder artikel 13 komt te vallen. Wij menen dat de meest eenvoudige en meest natuurlijke vorm van communicatie, het normale gesprek, niet buiten het bereik mag vallen van een grondwetsbepaling die in algemene zin vertrouwelijke communicatie wil beschermen. Het zou weinig consequent zijn om het telefoongesprek wel onder artikel 13 te rekenen, maar het gesprek dat zonder telecommunicatiemiddelen wordt gevoerd, niet.
Ook de praktische kant weegt hier zwaar. De moderne techniek heeft het in toenemende mate mogelijk gemaakt om gewone gesprekken ongemerkt af te luisteren. In reactie op de technische ontwikkelingen is het afluisteren van gesprekken met een technisch hulpmiddel strafbaar gesteld, terwijl het afluisteren door overheidsorganen sterk is gereguleerd (artikelen 139a en 139b Wetboek van Strafrecht). Met de voorgestelde uitbreiding van artikel 13 wordt aan deze bepalingen een grondwettelijke verankering gegeven die specifieker is dan het meer algemene artikel 10 Grondwet.
Artikel 13 geeft bovendien in drie opzichten ruimere bescherming dan

artikel 10, eerste lid. Artikel 10 laat delegatie toe bij het beperken van het grondrecht, terwijl artikel 13 alleen bij wet kan worden beperkt. Artikel 13 heeft voorts als uitgangspunt dat alleen een bij wet aangewezen orgaan de beperking kan toestaan: in het bij de Kamer ingediende voorstel wordt het orgaan bij de wet bepaald, in de nota van wijziging die deze nota vergezelt laat de Grondwet nog slechts de keuze tussen de rechter en – in zeer bijzondere gevallen – de minister. Artikel 10 laat de wetgever vrij in het aanwijzen van organen die beperkingen kunnen maken. Het derde verschil is dat artikel 13 de verplichting inhoudt om de betrokkene van de beperking in kennis te stellen.
Dit alles afwegende menen wij dat er goede gronden zijn om het vertrouwelijke gesprek onder de beschermende werking van artikel 13 te brengen. In een techniek-onafhankelijke benadering past het ook de vertrouwelijke communicatie zonder technische hulpmiddelen te beschermen. Wij denken dat dit een van de waardevolle punten is van het voorstel.

1.6. Overige vragen en opmerkingen

De leden van de PvdA-fractie onderschreven het belang om artikel 13 aan te passen aan de veranderende technologische mogelijkheden, maar vroegen zich af of de voorgestelde snelle aanpassing de juiste is. Het leek hen gewenst eerst een maatschappelijke discussie of publiek debat te voeren over het onderwerp, waarbij zowel het democratische, juridische, veiligheids- als het economische belang van vertrouwelijke communicatie aan bod zou moeten komen. Zij vroegen hoe de regering denkt over de instelling van een staatscommissie.
Wij menen dat het voorstel tot wijziging van artikel 13 op zijn eigen merites kan worden beoordeeld. De strekking van het voorstel is juist om artikel 13 aan te passen aan de veranderende technologische mogelijkheden. Omdat dit doel door de meeste fracties wordt onderschreven, zijn wij van mening dat het voorstel kan worden behandeld zonder een bredere discussie af te wachten.

De leden van de PvdA-fractie vroegen of de regering kon ingaan op de publicatie van N. A. N. M. van Eijk in het Nederlands Juristenblad[1] en andere (juridische) publicaties die over het onderwerp zijn verschenen of binnenkort zullen verschijnen. Bij de beantwoording van deze vraag beperken wij ons tot publicaties uit de vakpers. Het gaat dan om artikelen van mr. N. A. N. M. van Eijk en prof. Mr. E. J. Dommering.
Het centrale punt in de kritiek van Van Eijk is, dat de gewone fax en E-mail vogelvrij zijn. Dit punt hebben wij in paragraaf 1.2 en 1.3 uitvoerig besproken: wij delen de kritiek van Van Eijk niet. De stelling van deze auteur dat beeldinformatie buiten het bereik van artikel 13 valt is in paragraaf 1.4 vergaand genuanceerd. Artikel 13 heeft, zo concluderen wij, een veel ruimere strekking dan Van Eijk meent. Wij hebben dan ook geen behoefte aan de suggestie van deze auteur om eerst een bredere discussie te starten over een mogelijke herziening van de fundamentele vrijheden binnen het informatierecht. Een ander onderwerp dat Van Eijk aansnijdt, de rechterlijke last bij het beperken van het briefgeheim, komt hierna aan de orde (paragraaf 2.2). De kritiek van Dommering wordt hierna, in paragraaf 2.1, besproken.

De leden van de CDA-fractie hebben gevraagd of de regering heeft overwogen de bescherming van de bestaande communicatiemiddelen te handhaven en daarnaast bescherming van nieuwe communicatiemiddelen te regelen. Zij verwezen naar de systematiek van artikel 7 Grondwet. Deze variant is inderdaad overwogen, maar er is bewust van afgezien. De opzet van het nieuwe artikel 13 is, in algemene zin bescherming te verlenen aan vertrouwelijke communicatie, ongeacht de gekozen vorm.

[1] N. A. N. M. van Eijk, «(G)een recht op vertrouwelijke communicatie: fax en email vogelvrij,» *Nederlands Juristenblad* 19 september 1997, p. 1554–1555.

Daarbij staat de bedoeling voorop om de communicatievormen die nu in artikel 13 worden genoemd, onverminderd onder de bescherming van het nieuwe artikel te handhaven; daarover mag geen twijfel bestaan. De discussies over de reikwijdte van het nieuwe artikel, nu en in de toekomst, gaan alleen over nieuwe of nieuwere communicatievormen, waarover de opvattingen nog niet zijn uitgekristalliseerd. Een tweede argument is dat het niet bij het karakter van de Grondwet past om alle verschillende typen van beschermenswaardige communicatiemiddelen te vermelden, met name niet nu het om een veel groter aantal gaat dan de drie middelen die nu in de Grondwet worden genoemd. Wij concluderen dat er geen reden is om de aparte vermelding van drie specifieke vormen van communicatie te handhaven. Brief, telefoon en telegraaf verschillen immers niet wezenlijk van andere communicatievormen.

De leden van de SGP-fractie hebben (bij de bespreking van het eerste lid in het verslag) een vraag gesteld met tegengestelde strekking: moet het techniek-onafhankelijk maken van de grondwettelijke bescherming niet ook leiden tot veranderingen in artikel 7, waar gesproken wordt over drukpers, radio en televisie? Wij hebben toegezegd onderzoek te doen naar eventuele wijziging van artikel 7.[1] Het is nu nog niet mogelijk op de uitkomsten daarvan vooruit te lopen. Wel kan in dit stadium worden gewezen op een wezenlijk verschil tussen artikel 7 en artikel 13. Het recht van vrije meningsuiting is volgens vaste jurisprudentie opgebouwd uit een recht om meningen te openbaren en een recht om meningen te verspreiden. Het verspreidingsrecht wordt uitgeoefend door zogeheten verspreidingsmiddelen, die in sterke mate zijn gebonden aan bepaalde technieken. Sommige verspreidingsmiddelen brengen een ruimere reguleringsbehoefte van de overheid met zich dan andere. Dit aspect kan er toe leiden dat de bescherming die artikel 7 biedt wordt gedifferentieerd al naar gelang het middel van verspreiding, zodat bij sommige verspreidingsmiddelen voldoende ruimte wordt gecreëerd voor betrekkelijk vergaande regulering, terwijl bij die verspreidingsmiddelen waar de noodzaak voor regulering gering is, de Grondwet ook geringe ruimte voor regulering laat. Bij artikel 13 is een dergelijk sterk onderscheid tussen communicatiemiddelen niet nodig. De reguleringsbehoefte van de overheid bij de verschillende technieken van vertrouwelijke communicatie is niet van dien aard dat deze verschillende technieken ook in de Grondwet tot uitdrukking zouden moeten blijven komen.
Het voorgaande laat uiteraard onverlet dat artikel 7 geactualiseerd zou kunnen worden in het licht van nieuwe technologieën. Het onderzoek dat wij hebben toegezegd betreft ook dit aspect.

Het leek de leden van de CDA-fractie niet verstandig nu een nieuwe regelingsopdracht in de Grondwet op te nemen, nu de regering er niet in was geslaagd wetsvoorstellen inzake de bescherming van persoonsgegevens tijdig bij de Tweede Kamer in te dienen. Het wetsvoorstel bescherming persoonsgegevens is inderdaad niet, zoals aanvankelijk beoogd, voor 1 juni 1997 bij de Tweede Kamer ingediend. De voorbereiding van het voorstel, het uitbrengen van adviezen en de verwerking daarvan bleken meer tijd te kosten dan aanvankelijk was voorzien. Het ziet er thans naar uit dat het wetsvoorstel uiterlijk in december kan worden ingediend, nu de Raad van State zijn advies op 15 oktober heeft uitgebracht.

De vraag van de leden van de CDA-fractie over de kennisgevingsplicht wordt in paragraaf 4 beantwoord.

De leden van de RPF-fractie vroegen of de voorgestelde wijziging gevolgen heeft voor mogelijke controle op het Internetverkeer. In hoeverre ontstaat hierdoor een betere wettelijke basis om bijvoorbeeld racistische

[1] Handelingen II 1995/96, blz. 956.

of kinderpornografische uitingen op Internet op te sporen en degenen die dit op het net hebben gezet, te vervolgen, wilden deze leden weten.
Het wetsvoorstel heeft geen invloed op de mogelijkheden om racistische of kinderpornografische uitingen op Internet op te sporen. Bij de mogelijkheden om deze uitingen op te sporen moet onderscheid worden gemaakt tussen gegevens die via Internet worden getransporteerd enerzijds, en de opslag van gegevens die via Internet raadpleegbaar zijn anderzijds. Wanneer het alleen gaat om het transport, dan zullen de bepalingen over aftappen van telecommunicatie van toepassing zijn. Wanneer het echter gaat om gegevens die via Internet raadpleegbaar zijn, zullen de bepalingen die verband houden met huiszoeking in een computeromgeving van toepassing zijn, inclusief de in dat verband aanwendbare aparte bevoegdheid tot onderzoek via een netwerk, zoals neergelegd in artikel 125j van het Wetboek van Strafvordering. Dit artikel is een bepaling in de zin van het voorgestelde artikel 13 van de Grondwet, voorzover daarmee bijzondere procedurele waarborgen zijn gegeven indien toegang wordt verkregen met het oog op raadpleging van opgeslagen vertrouwelijke communicatie. Deze bepalingen maken het ook mogelijk om racistische en kinderpornografische uitingen op Internet, of andere uitingsdelicten, op te sporen, althans voorzover dit mogelijk is binnen de Nederlandse rechtsmacht.

2. Het eerste lid

2.1. Het begrip «vertrouwelijke communicatie»

De leden van de PvdA-fractie hebben opgemerkt dat het begrip «vertrouwelijke communicatie» is ontleend aan het proefschrift van J.A. Hofman. Zij hebben gevraagd of de regering heeft kennisgenomen van het commentaar op het proefschrift in *Mediaforum* 1996–2, en of de auteur van het proefschrift heeft meegewerkt aan de totstandkoming van het wetsvoorstel.
Wij zijn met de recensie van prof. Dommering in *Mediaforum* 1996–2 bekend. Het proefschrift van J.A. Hofman heeft ons geïnspireerd tot het herzien van artikel 13 en het centraal stellen van het begrip «vertrouwelijke communicatie». Dat betekent niet dat het proefschrift bepalend is geweest voor de inhoud van het wetsvoorstel. De auteur is slechts zeer zijdelings betrokken geweest bij de opstelling ervan: een eerste concept van het ontwerp is hem voor commentaar voorgelegd. Dat betekent ook dat het artikel dat Dommering als commentaar op het wetsvoorstel heeft geschreven[1] op dit moment relevanter is dan zijn proefschriftrecensie uit 1996.
In dit recentere artikel wordt het criterium «geobjectiveerde wil tot vertrouwelijkheid» bekritiseerd. De schrijver stelt als alternatief criterium voor dat het bericht moet zijn geadresseerd. Dit criterium, dat ook door de leden van de VVD-fractie als mogelijkheid is genoemd, verschilt niet zo veel van het criterium dat wij hebben voorgesteld. Uit de adressering zal immers in veel gevallen de wil tot vertrouwelijkheid blijken. Toch geven wij de voorkeur aan het eigen criterium: de geobjectiveerde wil van de verzender dient bepalend te zijn. Die wil kan voldoende blijken uit de adressering, maar adressering is niet altijd genoeg. Afhankelijk van het gekozen communicatiemiddel mag van de verzender ook een zekere inspanning worden gevergd om de vertrouwelijkheid zichtbaar te maken. Dat geldt niet voor telefoon, maar het geldt wel bij post. Adressering is ook daarom niet genoeg omdat de opsteller een boodschap soms ruimer verspreidt dan aan de geadresseerde alleen; men denke aan de open brief. Dommering meent dat een geadresseerde ansichtkaart door artikel 13 moet worden beschermd; wij delen dit standpunt niet. Van de afzender mag toch nog wel verwacht worden dat hij een brief in een envelop stopt. Een postbode kan zelfs per ongeluk een ansichtkaart lezen, omdat zijn oog

[1] Egbert Dommering, «Geen telefoongeheim op de elektronische snelweg», in *Mediaforum* 1997-10.

erop valt. Het is moeilijk vol te houden dat hij dan nog een hindernis moet nemen.
Dommering vat het recht op vertrouwelijke communicatie met zoveel woorden op als een «transportrecht». De leden van de D66-fractie hebben voorgesteld een «transportgeheim» te introduceren. Wij achten deze benadering te beperkt. Het is enigszins gekunsteld om zoals Dommering doet een brief die is bezorgd maar nog niet is geopend onder een dergelijk transportrecht of transportgeheim te brengen. De brief is immers getransporteerd. In het concept van «vertrouwelijke communicatie» is het daarentegen passend dat ook in deze fase de brief nog wordt beschermd. Een tweede aspect betreft het vertrouwelijke gesprek. Wij rekenen dit onder het begrip «vertrouwelijke communicatie»; als artikel 13 alleen wordt opgevat als een transportrecht, is dat niet mogelijk.

De leden van de PvdA-fractie hebben geconcludeerd dat voor normaal verzonden E-mail geen grondwettelijke bescherming zal gelden. Zij deelden het standpunt van de regering niet. De leden van de CDA-fractie vonden dit standpunt niet aanvaardbaar. Zij stelden dat de regering door te goochelen met het begrip «geobjectiveerde wil» tot een vergaande beperking van de bescherming van vertrouwelijke communicatie komt. De leden van de VVD-fractie stelden soortgelijke vragen.
In het algemeen gedeelte van deze nota is uitvoerig stilgestaan bij het begrip «vertrouwelijke communicatie», en meer specifiek bij faxverkeer en E-mail. Wij hebben daar getracht aan te geven dat het begrip «vertrouwelijke communicatie» een ruime inhoud heeft, zodat van gegoochel geen sprake is. Met name hebben wij betoogd dat E-mail in vrijwel alle gevallen wordt beschermd. Wij hopen dat met deze uiteenzetting de vrees van de genoemde leden is weggenomen.

De leden van de PvdA-fractie vroegen of het juist is de verkeersgegevens buiten de werking van artikel 13 te houden. De leden van de CDA-fractie waren het niet met de regering eens dat verkeersgegevens fundamenteel verschillen van het type informatie dat verkregen wordt bij de interceptie van de inhoud van vertrouwelijke communicatie. Zij verwezen naar de uitspraak van het Europese Hof voor de Rechten van de Mens (EHRM) in de zaak Malone. De leden van de GPV-fractie vonden het onderscheid dat wordt gemaakt tussen de inhoud van vertrouwelijke communicatie en verkeersgegevens tamelijk geforceerd.
De uitspraak van het EHRM in de Malone-zaak[1] is, waar het gaat om verkeersgegevens[2], voor meerdere uitleg vatbaar. Enerzijds stelt het Hof dat de verkeersgegevens van telefoongesprekken te onderscheiden zijn van de inhoud van het gesprek, anderzijds dat verkeersgegevens gegevens bevatten die een integraal onderdeel uitmaken van de telefoongesprekken zelf. De uitspraak van het Hof geeft dus geen duidelijke richting. De benadering die het Hof kiest moet echter ook in zijn context worden bezien. Artikel 8 van het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele Vrijheden (EVRM) beschermt privé-leven en correspondentie in gelijke mate. Onder welk van de twee verkeersgegevens worden gerekend, is dus minder relevant voor de bescherming die van artikel 8 EVRM uitgaat. In de Grondwet is hetgeen artikel 8 EVRM beschermt, verdeeld over twee artikelen met verschillende mate van bescherming: vertrouwelijke communicatie (artikel 13) wordt sterker beschermd dan de persoonlijke levenssfeer (artikel 10). Het heeft onze voorkeur om vast te houden aan het onderscheid tussen de eigenlijke communicatie en verkeersgegevens. Dit onderscheid wordt ook in de huidige wetgeving al gehanteerd. De officier van justitie kan bij voorbeeld in het kader van de opsporing inlichtingen opvragen over het verkeer dat over een openbaar telecommunicatienetwerk heeft plaatsgevonden, mits aan enkele vereisten is voldaan (artikel 125f). Om echter

[1] Malone, Europees Hof voor de Rechten van de Mens, 2 augustus 1984, Series A, no. 82, paragraaf 84.
[2] Verkeersgegevens zijn gegevens over gevoerde communicatie. Bij telefoongesprekken gaat het om dag, tijdstip en duur van gevoerde gesprekken, en de nummers of namen van de deelnemers.

gesprekken te kunnen aftappen is een beslissing van de rechter-commissaris vereist (artikel 125g).

De leden van de PvdA-fractie informeerden wat de status is van de inloggegevens bij E-mail, waaronder de onderwerpsaanduiding in de kop van het bericht. Wij menen dat de inloggegevens onder de verkeersgegevens moeten worden gerekend, maar de kop van het bericht niet. Ook vroegen deze leden in welke gevallen artikel 10 Grondwet van toepassing is op verkeersgegevens, in welke gevallen artikel 13 en in welke gevallen de verkeersgegevens niet zijn beschermd. De inhoud van de communicatie wordt, zoals in paragraaf 1 uiteengezet, beschermd door artikel 13 Grondwet. Verkeersgegevens worden altijd beschermd door artikel 10, eerste lid, Grondwet, omdat zij tot de persoonlijke levenssfeer kunnen worden gerekend. Zijn de verkeersgegevens opgenomen in een geautomatiseerde of systematisch aangelegde registratie, dan is ook de krachtens artikel 10, tweede en derde lid, Grondwet vastgestelde Wet persoonsregistraties van toepassing. Gegevens over telefoongesprekken en andere communicatie over het telefoonnet zullen in de praktijk vrijwel steeds in een persoonsregistratie zijn opgenomen.

De leden van de VVD-fractie, evenals die van de D66-fractie, hebben gevraagd of het telefoongeheim vervalt wanneer iemand een telefoongesprek voert met het telefoonapparaat op de speaker. Het antwoord is ontkennend. Artikel 13 beschermt de transportfase over het telefoonnet; het gebruik van een speaker heeft daarop geen invloed. Eerder geldt het omgekeerde: het gebruik van een speaker kan een inbreuk betekenen op de persoonlijke levenssfeer van de persoon aan de andere kant van de lijn. Daarvan is sprake wanneer de spreker aan de andere kant van de lijn niet weet dat een onbekende derde het gesprek via de speaker kan volgen, en hij dat ook niet hoeft te verwachten. Omdat speakers op dit moment weinig worden gebruikt, hoeft een beller, met name bij privé-gesprekken, meestal niet bedacht te zijn op het gebruik van een speaker. In het zakelijk verkeer kan dit in bepaalde gevallen anders liggen. Wie meent dat zijn privacy is geschonden kan zich wenden tot de burgerlijke rechter op grond van onrechtmatige daad.

De leden van de VVD-fractie hebben voorgesteld het criterium «geobjectiveerde wil tot vertrouwelijkheid» te vervangen door het criterium dat de informatie moet zijn geadresseerd. Op dit onderwerp is eerder in deze paragraaf ingegaan.

De leden van de D66-fractie menen, in reactie op een opmerking in de memorie van toelichting, dat het gebruik van compressietechnieken niets te maken heeft met het coderen van berichten. Wij kunnen deze leden toegeven dat compressietechnieken zijn ontworpen om de hoeveelheid gegevens die verstuurd moet worden te verminderen. Dat neemt niet weg deze technieken ook gebruikt kunnen worden om het aftappen moeilijker te maken. Het rechtstreeks volgen van een telefoongesprek is immers bij het gebruik van compressie niet mogelijk.

De leden van D66 vroegen of de zwaardere vormen van versleuteling zullen worden toegestaan. In het tweede voortgangsrapport over het nationale actieplan elektronische snelwegen hebben wij meegedeeld dat wij geen voornemens hebben om particulieren voor eigen gebruik de mogelijkheden voor versleuteling te ontzeggen. Daar er geen regeling is – en het ook niet onze bedoeling is een regeling te maken – die gebruik van zulke technieken verbiedt, is dit dus toegestaan. Dit standpunt laat onverlet dat wordt gezocht naar mogelijkheden om het aanbod van zulke technieken op de markt te reguleren. Daar waar echter nu, bijvoorbeeld

via Internet, verschillende technieken door particulieren kunnen worden verkregen, blijft dit in de toekomst ook gewoon mogelijk.

De leden van GPV-fractie hebben opgemerkt, het een groot probleem te vinden dat uit de tekst van het nieuwe artikel 13 niet duidelijk is wat onder vertrouwelijke communicatie moet worden verstaan. Weliswaar wordt in de toelichting getracht daaraan inhoud en begrenzing te geven, maar deze toelichting kan, zo betoogden deze leden, hooguit dienen voor de wetgever als enige indicatie ter nadere uitwerking.
De strekking van het wetsvoorstel is niet om de bestaande begrippen te vervangen door een onduidelijk begrip, maar om ze te vervangen door een ruimer begrip. Het briefgeheim en het telefoonen telegraafgeheim blijven zonder meer onder de werking van artikel 13. Gekozen is voor een techniek-onafhankelijke opzet, alleen al om te voorkomen dat de Grondwet bij iedere technische ontwikkeling achter gaat lopen. Wijziging van de Grondwet is immers een tijdrovende operatie. Met het introduceren van het begrip «vertrouwelijke communicatie» is dus verzekerd dat de Grondwet haar beschermende werking kan uitoefenen zodra zich een nieuwe ontwikkeling op het gebied van de communicatie voordoet.

2.2. Beperkingsclausule

Beperking van het briefgeheim is thans alleen mogelijk op last van de rechter. Wij hebben voorgesteld dit vereiste niet in de Grondwet zelf meer op te nemen, omdat het traditionele onderscheid tussen het briefgeheim en andere vormen van communicatie komt te vervallen.
De leden van de PvdA-fractie wezen op de memorie van toelichting, waarin is aangegeven dat de rechter in de meeste gevallen de meest gerede instantie is om toestemming te geven voor beperking van de vertrouwelijkheid van communicatie. Waarom, zo vroegen deze leden, heeft de regering er dan niet voor gekozen om, zoals de Raad van State aanbeveelt, dit in de Grondwet vast te leggen? Hierbij zou dan een uitzonderingsbepaling voor de veiligheidsdienst kunnen worden opgenomen. De leden van de CDA-fractie zagen geen noodzaak, na de discussie daarover bij de grondwetsherziening van 1983, het vereiste van een rechterlijke last te laten vallen. De leden van de fractie van D66 waren verbaasd over het verlaten van het principe dat alleen op last van de rechter inbreuk gemaakt kan worden op het grondrecht van vertrouwelijke communicatie. De leden van de GPV-fractie waren niet overtuigd door de argumenten van de regering voor een in de formele wet op te nemen beperkingsclausule, waardoor eventueel ook een andere instantie dan de rechter kan worden aangewezen. Zij waren het er niet mee eens dat hierdoor in feite de huidige stand van zaken zal worden bestendigd. Deze leden konden zich nog wel voorstellen dat het specifieke karakter van de inlichtingen- en veiligheidsdiensten om een specifieke oplossing vraagt, maar, zo merkten zij op, de tekst van het voorgestelde artikel biedt ook ruimte aan allerlei andere uitzonderingen op de regel.
Wij hechten aan het uitgangspunt dat bij een algemeen omschreven grondrecht ook een algemene beperkingsclausule past. Wel geven de vragen en opmerkingen ons aanleiding om de tekst van artikel 13 bij nota van wijziging aan te vullen, zodat de uitgangspunten die in de toelichting zijn uiteengezet, ook uitdrukkelijk in de Grondwet zijn terug te vinden. Als hoofdregel wordt neergelegd dat beperking van het grondrecht alleen mogelijk is op last van de rechter. Bij de wet kan echter worden bepaald dat een beperking mogelijk is met machtiging van een bij de wet aangewezen minister. Deze uitzonderingsmogelijkheid wordt uitsluitend gecreëerd met het oog op de taakuitoefening van de diensten bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten. In artikel 13 zelf wordt dit tot uitdrukking gebracht door het te binden aan het criterium «het belang van de nationale veiligheid».

Wanneer de taakuitoefening van de inlichtingen- en veiligheidsdiensten in het geding is, is niet de rechter maar de minister het aangewezen orgaan, om de volgende redenen. Het gaat om een werkzaamheid die een onderdeel is van de totale nationale veiligheid en die derhalve slechts kan worden uitgeoefend in het kader van het beleid op dat gebied in zijn geheel. De beslissing om al dan niet een inbreuk op vertrouwelijke communicatie te maken is een belangrijke beleidsbeslissing die in een dergelijke situatie verband houdt met de nationale veiligheid. De verantwoordelijkheid daarvoor dient bij een minister te liggen. Voorts zal de minister doorgaans beter geïnformeerd zijn dan de rechter, hetgeen zwaar weegt nu de betrokkene niet kan worden gehoord. Tenslotte is er een belangrijk verschil met procedures in het kader van strafvordering: bij strafvorderlijke procedures is de rechter zelf verantwoordelijk voor de gehele procedure; bij een onderzoek door een inlichtingen- en veiligheidsdienst is de minister verantwoordelijk.[1]
Het criterium «nationale veiligheid» vormt een van de gronden waarop het in artikel 8 EVRM neergelegde grondrecht kan worden beperkt. In de jurisprudentie van het Europese Hof en de Europese Commissie voor de Rechten van de Mens komt bovendien naar voren dat de activiteiten van inlichtingen- en veiligheidsdiensten, waarmee inbreuken op artikel 8 EVRM worden gemaakt, bij uitstek aan deze beperkingsgrond worden getoetst.
Door de woorden «bij de wet» is bovendien vastgelegd dat op dit punt delegatie niet mogelijk is. De woorden «een bij de wet aangewezen minister» laten overigens naar onze mening toe dat de wet als eis stelt dat de machtiging moet worden verleend door twee of meer ministers gezamenlijk.
Deze wijziging is neergelegd in de bijgevoegde nota van wijziging.
Deze nota van wijziging betekent dat, niet slechts voor het briefgeheim maar voor alle vormen van vertrouwelijke communicatie, als hoofdregel zal gelden dat beperking alleen op rechterlijke last kan geschieden. Deze hoofdregel wordt nu in de Grondwet vastgelegd. Op dit punt betekent het voorstel een versterking van de waarborgfunctie van de Grondwet, met name ook voor het telefoon- en telegraafgeheim, maar vanzelfsprekend ook voor modernere vormen, zoals persoonlijk gerichte E-mail en faxverkeer gedurende de verzending.

De leden van de PvdA-fractie meenden dat de regering voorstelt alsnog de wijziging aan te brengen die bij de grondwetsherziening van 1983 door een amendement van het lid Bakker niet is doorgevoerd. De leden van de SGP-fractie vroegen om aan de hand van de grondwetsgeschiedenis aan te geven of de argumenten die destijds golden om voor het briefgeheim een sterkere bescherming voor te schrijven nu niet meer van toepassing zijn.
De grondwetsgeschiedenis is als volgt. Het briefgeheim is in 1848 in de Grondwet opgenomen. Deze bepaling stelde al vanaf het begin de eis dat beperking alleen op last van de rechter mogelijk is. Bij de grondwetsherziening van 1983 werd de bepaling uitgebreid met het telefoon- en telegraafgeheim. De regering koos aanvankelijk voor een uniforme regeling, waarbij het brief-, telefoon- en telegraafgeheim alleen konden worden beperkt «door of met machtiging van hen die daartoe bij [de] wet zijn aangewezen». Daarop diende het lid Bakker een amendement in (kamerstukken II 1976/77, 13 872, nr. 20), dat de strekking had, de bestaande waarborg voor het briefgeheim te handhaven. Het amendement had geen betrekking op het telefoon- en telegraafgeheim, omdat de wetgeving het afluisteren van telefoongesprekken met het oog op de staatsveiligheid mogelijk maakt zonder rechterlijke last (Handelingen II 1976/77, blz. 2208). Na aanvankelijk verzet werd dit amendement door de regering overgenomen.

[1] Kamerstukken II 1966/67, 8911, nr. 3, blz. 7–8; 1969/70, 9419, nr. 4, blz 3; idem nr. 8, blz. 3.

Het verschil ten opzichte van 1983 is gelegen in de opzet en systematiek van het nieuwe artikel 13. De huidige tekst van het artikel noemt drie vormen van telecommunicatie. In die opzet past het dat, voor elke communicatievorm afzonderlijk, wordt afgewogen of in alle gevallen een rechterlijke last kan worden verlangd. In de nieuwe opzet, waarin afzonderlijke vormen van vertrouwelijke communicatie niet meer worden genoemd, is een dergelijke benadering niet goed meer mogelijk. Dit neemt niet weg dat de wet thans geen inperkingen van het briefgeheim mogelijk maakt zonder rechterlijke last. Wij delen het standpunt van de leden van de PvdA-fractie dan ook niet.

De leden van de PvdA-fractie verwezen naar de uitspraak van het EHRM in de Klass-zaak[1] en de uitleg die de Raad van State aan die uitspraak heeft gegeven. In deze uitspraak, zo geven zij aan, komt naar voren dat het wenselijk is om voorafgaand aan, tijdens en na afloop van een onderzoek de toetsing op te dragen aan een rechter. De regering stelt echter, zo vervolgen deze leden, dat het in overeenstemming is met deze uitspraak om aan de formele wetgever de ruimte te laten om te bepalen dat onder omstandigheden een andere instantie dan de rechter bevoegd is tot het verlenen van een machtiging. Kan de regering nader ingaan op het verschil van interpretatie met de Raad van State, zo vroegen zij.
De Raad van State leidt uit het Klass-arrest af dat het wenselijk is om voorafgaand aan, tijdens en na afloop van een onderzoek de toetsing op te dragen aan de rechter.[2] De rechterlijke toetsing na afloop van het onderzoek komt hierna nog aan de orde, in paragraaf 4. Ten aanzien van de toetsing voorafgaand aan en tijdens het onderzoek wordt in het Klass-arrest vooropgesteld dat het in beginsel wenselijk is dat het toezicht op onderzoeken waarbij brieven geopend of telefoons afgetapt kunnen worden, wordt opgedragen aan een rechter. In de wetgeving van de Bondsrepubliek ontbrak dergelijk toezicht, maar er was wel voorzien in een zware vorm van bestuurlijk en politiek toezicht, door een commissie bestaande uit vijf (inmiddels negen) leden van de Bundestag, inclusief leden van de oppositie, en een onafhankelijke commissie, benoemd door de parlementaire commissie. Deze organen beschikten, zo stelde het Hof, over voldoende bevoegdheden om een effectief toezicht te kunnen uitoefenen. Het Hof achtte dit voldoende (paragraaf 56).
Om te kunnen beoordelen of het Nederlandse stelsel van toezicht, zoals dat zal worden neergelegd in de ontwerp-Wet op de inlichtingen- en veiligheidsdiensten, voldoende effectief is om het ontbreken van rechterlijk toezicht te kunnen rechtvaardigen, is het ook van belang om dit stelsel te vergelijken met het toezichtstelsel dat in het Verenigd Koninkrijk bestaat. De Europese Commissie voor de Rechten van de Mens heeft namelijk geoordeeld dat het ontbreken van rechterlijke toetsing bij het optreden van veiligheidsdiensten in het Verenigd Koninkrijk geen strijd met artikel 8 EVRM oplevert, omdat zij het Britse toezichtstelsel voldoende effectief achtte.[3] In de ontwerp-Wet op de inlichtingen- en veiligheidsdiensten, die binnenkort bij de Tweede Kamer zal worden ingediend, wordt een nieuw stelsel van toezicht op de inlichtingen- en veiligheidsdiensten geïntroduceerd. Het Britse stelsel van toezicht[4] kent twee toezichtsorganen: een Tribunaal en een Commissioner. De leden van het Tribunaal worden door de Kroon benoemd. Zij kunnen ook alleen door de Kroon uit hun functie worden ontheven, op een verzoek namens de beide Huizen van het Parlement. De Commissioner wordt benoemd door de Minister-President. Het Tribunaal behandelt klachten van burgers, die van mening zijn dat ten onrechte een onderzoek naar hen is of wordt verricht door de Security Service. Als de klacht ontvankelijk is verklaard, verricht de Commissioner het inhoudelijke onderzoek. Het Tribunaal kan tot het oordeel komen dat er geen redelijke grond was om het onderzoek te verrichten; deze toetsingsnorm komt ongeveer overeen met wat in het Nederlandse bestuursrecht bekend staat als marginale toetsing. In dat

[1] Klass en anderen, Europees Hof voor de Rechten van de Mens, 6 september 1978, Series A, no. 28 (1979).
[2] Kamerstukken II 1996/97, 25 443, B, punt 2.
[3] Zaken 18 601/91, D.E. v. Verenigd Koninkrijk, 20 317/92, Hewitt & Harman v. Verenigd Koninkrijk, en 20 271/92, Redgrave v. Verenigd Koninkrijk.
[4] De tweede ondergetekende heeft de Kamer op 19 december 1996 doen toekomen een overzicht van parlementaire controlestelsels op de geheime diensten in een aantal West-Europese landen (Kamerstukken II 1996/97, 24 174, nr. 4). Voor een meer uitvoerige beschrijving van het Britse stelsel van toezicht verwijzen wij kortheidshalve naar dat overzicht.

geval kan het Tribunaal bepalen dat het onderzoek, zo het nog loopt, wordt gestaakt, en het Tribunaal kan de Minister van Binnenlandse Zaken schadevergoeding opleggen. De beslissing van het Tribunaal is definitief, beroep op de rechter is expliciet uitgesloten. De Commissioner schrijft jaarlijks een rapport aan de Minister-President; die legt dit – eventueel ontdaan van gevoelige informatie – voor aan het Parlement.
In het ontwerp-Wet op de inlichtingen- en veiligheidsdiensten wordt het onafhankelijke toezicht op de inlichtingen- en veiligheidsdiensten opgedragen aan een commissie van toezicht. De leden zullen worden benoemd en ontslagen door de Kroon. De taak van de commissie van toezicht is: (1) het toezicht op de rechtmatigheid van de uitvoering van hetgeen bij of krachtens de Wet op de inlichtingen- en veiligheidsdiensten en de Wet Veiligheidsonderzoeken is gesteld en (2) het onderzoeken en beoordelen van klachten.
Het toezicht betreft toezicht achteraf. De uitoefening van bevoegdheden is dus niet afhankelijk van een vorm van instemming door de commissie vooraf. Als de commissie in het kader van haar toezichthoudende taak een onderzoek verricht, legt zij haar bevindingen neer in een rapport, dat zij uitbrengt aan de minister. Dit rapport wordt, met de reactie van de minister, voorgelegd aan de commissie voor de inlichtingen- en veiligheidsdiensten van de Tweede Kamer. De minister kan dan door deze commissie ter verantwoording worden geroepen.
De klachtenprocedure bij de commissie van toezicht komt in de plaats van de procedure bij de Nationale ombudsman. De procedure is in grote lijnen gelijk aan de procedure die nu al geldt bij de Nationale ombudsman. Het oordeel van de commissie over de klacht wordt aan de minister uitgebracht; de commissie kan eventueel ook aanbevelingen doen. Het oordeel van de commissie, haar eventuele aanbevelingen alsmede de reactie van de minister worden ter kennis gebracht van de commissie voor de inlichtingen- en veiligheidsdiensten van de Tweede Kamer.
In vergelijking met het Britse stelsel, dat de toets van de Europese Commissie heeft weten te doorstaan, vertoont het voorgestelde Nederlandse stelsel enkele pluspunten. Het Britse Tribunaal onderzoekt alleen klachten; de Nederlandse commissie oefent ook eigener beweging toezicht uit. Verder wordt het eigenlijke onderzoek in het Britse systeem verricht door de Commissioner, die niet voldoet aan alle eisen van onafhankelijkheid, terwijl in Nederland het onderzoek zal worden verricht door de onafhankelijke commissie van toezicht zelf. Wij gaan er dan ook van uit dat de voorgestelde structuur en werkwijze past binnen artikel 8 EVRM en de uitleg die het Europese Hof en de Europese Commissie daaraan hebben gegeven, omdat het ontbreken van rechterlijke toetsing wordt ondervangen door de instelling van een orgaan dat over voldoende bevoegdheden beschikt om een effectief toezicht te kunnen uitoefenen.

De vragen van de leden van de SGP-fractie over beeldinformatie zijn hiervoor, in paragraaf 1.4, beantwoord.

De leden van de CDA-fractie vroegen of het wetsvoorstel bijzondere opsporingsbevoegdheden (25 403) aan het voorstel tot wijziging van de Grondwet is getoetst. Dit is inderdaad het geval. Het wetsvoorstel bijzondere opsporingsbevoegdheden regelt in de wet de inbreuken op grondrechten door de politie in veel verdergaande mate dan tot dusverre het geval was. De ontwikkelingen in de informatietechnologie leiden tot twee flankerende ontwikkelingen in het recht. Enerzijds wordt de bescherming van de burger uitgebreid, gelet op de bedreigingen van de persoonlijke levenssfeer door de technische ontwikkelingen. Anderzijds worden de bevoegdheden van de politie om met het oog op de opsporing van strafbare feiten inbreuken te maken op de rechten van de burger ook uitgebreid, zij het met gelijktijdige opneming van waarborgen tegen misbruik ervan: inhoudelijke criteria, alsmede bijzondere procedurele waarborgen

wat betreft de toetsing aan deze criteria. De extra bescherming voor de burger bestaat in het wetsvoorstel bijzondere opsporingsbevoegdheden, in lijn met dit wetsvoorstel, onder meer uit een notificatieplicht ten aanzien van de uitoefening van bijzondere opsporingsbevoegdheden. Deze notificatieplicht is terug te vinden in artikel 126bb van het Wetboek van Strafvordering, zoals opgenomen in dat wetsvoorstel.

3. De regelingsopdracht (tweede lid, vernummerd tot derde lid)

De leden van de VVD-fractie hebben geconstateerd dat de nieuwe Telecommunicatiewet de data- en telefoondiensten liberaliseert, maar dat die wet nauwelijks ingaat op de vraag of het grondrecht directe of indirecte werking heeft in private verhoudingen (horizontale werking). Deze leden vroegen de regering daar alsnog een beschouwing over te geven.
In de jurisprudentie rond de horizontale werking van grondrechten is niet een heel duidelijke lijn te onderkennen, de rechter gaat, aldus Burkens[1], dogmatische problemen uit de weg. In hoeverre horizontale werking van het geldende artikel 13 moet worden aangenomen, en wat dat concreet betekent voor de oplossing van geschillen, wordt dan ook niet heel duidelijk. Het gemeenschappelijke element in de meeste uitspraken is dat de rechter een afweging maakt tussen het belang dat de een heeft bij de bescherming van zijn communicatie en het belang dat een ander heeft bij het kennisnemen daarvan. Omdat bij dit eerste belang doorgaans het grondrechtelijke aspect meeweegt, wordt de beperking van vertrouwelijke communicatie vaak getoetst aan de eisen van subsidiariteit en proportionaliteit. Het belang van horizontale werking is de laatste jaren toegenomen, enerzijds door de privatisering van het telefoonverkeer, anderzijds door de opkomst van nieuwe communicatietechnieken, die vooral door particulieren worden aangeboden.[2]
Wanneer de Grondwet alleen een vrijheidsrecht garandeert en de wetgever zich niet specifiek bezighoudt met de bescherming van dat recht in de relaties tussen burgers onderling, is de vraag van de horizontale werking primair een voor de rechter. De eventuele doorwerking van het grondrecht kan dan gestalte krijgen door de jurisprudentie.
De bescherming van vertrouwelijke communicatie is echter een onderwerp dat de wetgever zich nu al heeft aangetrokken. Er zijn diverse regelingen die bescherming verlenen in horizontale verhoudingen.
Met het nieuwe tweede lid (bij nota van wijziging vernummerd tot derde lid) wordt een regelingsopdracht gegeven aan de wetgever. Dat zal leiden tot een versterking van de werking van het grondrecht in horizontale relaties: de wetgever dient de bescherming van vertrouwelijke communicatie, ook in de relaties tussen burgers onderling, te verzekeren. Het betekent ook dat de wetgever voortaan tot taak heeft, te onderzoeken welke nieuwe vormen van vertrouwelijke communicatie er ontstaan, om vervolgens te bezien hoe deze nieuwe vormen beschermd moeten worden. Heeft de wetgever (nog) geen regels vastgesteld voor bepaalde nieuwe technieken, dan kan de rechter een aanvullende rol vervullen, waarbij hij gebruik kan maken van de algemene uitgangspunten van artikel 13. Dergelijke rechterlijke uitspraken kunnen dan weer een signaal zijn aan de wetgever.

De leden van de PvdA-fractie stelden dat naar hun mening in de ontwerp-Telecommunicatiewet nauwelijks garanties worden geboden voor E-mail. Zij vroegen, aan te geven hoe het elektronisch briefgeheim thans in het Wetboek van Strafrecht is geregeld, en hoe en wanneer de regering van plan is dit artikel aan te passen. Ook informeerden zij waarom hieraan in de nieuwe Telecommunicatiewet geen speciale aandacht is gegeven. De leden van de D66-fractie vroegen hoe de regering, met het verdwijnen van het post- en telecommonopolie, de onschendbaarheid van vertrouwelijk telefoonverkeer denkt te verzekeren.

[1] M. C. Burkens, *Algemene leerstukken van grondrechten naar Nederlands constitutioneel recht,* Zwolle 1989, p. 184–192.
[2] L. F. M. Verhey, *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy,* Zwolle 1992, p. 231–333. P. W. C. Akkermans, «Artikel 13», in P. W. C. Akkermans, A. K. Koekkoek, *De Grondwet. Een artikelsgewijs commentaar,* 2e druk 294–295. Zwolle 1992, P. J. A. Hofman, *Vertrouwelijke communicatie,* Amsterdam 1995, p. 131–132.

Wij menen dat de bescherming van vertrouwelijke communicatie bij de ontwerp-Telecommunicatiewet[1] wel degelijk de vereiste aandacht heeft gekregen. De Telecommunicatiewet heeft een brede doelstelling. De wet strekt ertoe de diversiteit van de telecommunicatievoorzieningen te verbeteren, de kwaliteit en toegankelijkheid van de telecommunicatie-infrastructuur te bevorderen, en een aantal maatschappelijke belangen bij toegang en gebruik te waarborgen. In de toelichting op het wetsvoorstel komt naar voren dat onder deze maatschappelijke belangen ook de bescherming van de persoonlijke levenssfeer van gebruikers wordt gerekend. Wij verwijzen naar de paragrafen 1.1.3 en 2.4 en met name naar paragraaf 6.3 van de memorie van toelichting bij de ontwerp-Telecommunicatiewet.
Het wettelijke beschermingsniveau dat door het nieuwe lid van artikel 13 wordt verlangd is voor een groot gedeelte gerealiseerd in de bestaande wetgeving, met name in de strafwetgeving. Met de ontwerp-Telecommunicatiewet wordt de bescherming nog op enkele punten uitgebreid.
In de nu geldende wetgeving is het verboden om opzettelijk wederrechtelijk binnen te dringen in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan (computervredebreuk, artikel 138a Wetboek van Strafrecht). Ook is het verboden gegevens af te tappen of op te nemen die zijn overgedragen door middel van de telecommunicatie-infrastructuur of via een telecommunicatie-inrichting die wordt aangewend voor dienstverlening aan het publiek (artikel 139c Wetboek van Strafrecht). Deze verbodsbepalingen hebben mede betrekking op E-mail, en zij richten zich in ieder geval tot derden. Er is twijfel mogelijk of de Internetprovider die kennis neemt van berichten in een mailbox op de server van de provider, computervredebreuk pleegt. Bij computervredebreuk is die twijfel hierin gelegen dat de server eigendom van de provider. Bij het tapverbod is het probleem dat het artikel betrekking heeft op gegevens*stromen,* niet op opgeslagen gegevens. Om op dit punt iedere twijfel uit te sluiten, zullen wij het Wetboek van Strafrecht aanvullen.
In artikel 19.11 van de Telecommunicatiewet worden de strafbepalingen vooral wetstechnisch aangepast. De artikelen 161sexies en 161septies Wetboek van Strafrecht worden bovendien zo aangepast dat het veroorzaken van storingen op Internet, bijvoorbeeld door het verzenden van zeer grote hoeveelheden gegevens naar een bepaalde elektronische brievenbus, een prikbord of ander adres strafbaar wordt gesteld.[2]

Ook op aanbieders van openbare telecommunicatienetwerken en aanbieders van openbare telecommunicatiediensten rust de taak om de privacy van de consumenten te beschermen. In de ontwerp-Telecommunicatiewet zijn daarom twee zorgplichtbepalingen opgenomen, die overigens materieel overeenkomen met de nu geldende regels: de aanbieders dienen zorg te dragen voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers (artikel 11.2). Zij dienen passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (artikel 11.3, eerste lid). De Minister van Verkeer en Waterstaat kan met betrekking tot de veiligheid en beveiliging regels stellen (artikel 18.8). Hij kan bovendien, in overeenstemming met de Minister van Justitie, aanwijzingen geven over de instandhouding, de exploitatie, het verzorgen en het gebruik van de telecommunicatiediensten en -netwerken (artikel 18.9).
Ook het personeel van de telecommunicatie-aanbieders dient het communicatiegeheim te respecteren. Het Wetboek van Strafrecht bevat een aantal bepalingen die dit gedetailleerd regelen (artikelen 371–375). Deze bepalingen zullen nader worden bezien en eventueel worden aangepast om te verzekeren dat zij zullen gelden voor het personeel van alle openbare telecommunicatie-aanbieders.

[1] Voorstel van wet houdende regels inzake de telecommunicatie (Telecommunicatiewet), kamerstukken II 1996/97, 25 533, nrs. 1–3.
[2] Kamerstukken II 1996/97, 25 533, nr. 3, blz. 143.

De Telecommunicatiewet bevat daarnaast meer specifieke bepalingen. Zo is de aanbieder van een openbare telecommunicatiedienst verplicht de abonnee op diens verzoek niet-gespecificeerde rekeningen te sturen (artikel 11.4). Voorts moeten de gegevens over het feitelijk gebruik van netwerken en diensten bij beëindiging van iedere oproep in beginsel worden verwijderd of geanonimiseerd (artikel 11.5), en kan een abonnee verlangen dat zijn persoonsgegevens niet in een telefoongids worden vermeld en niet aan derden worden verstrekt (artikel 11.6). Deze bepalingen strekken primair tot bescherming van de persoonlijke levenssfeer (artikel 10 Grondwet), maar kunnen indirect ook bijdragen aan een ongehinderd gebruik van voorzieningen voor vertrouwelijke communicatie.
De handhaving van deze bestuursrechtelijke en strafbepalingen berust bij de Onafhankelijke post- en telecommunicatieautoriteit. Dit college kan bestuursdwang uitoefenen en bestuurlijke boetes tot een bedrag van een miljoen gulden opleggen.

De leden van de D66-fractie vroegen hoe het komt dat er in Nederland zoveel meer wordt getapt dan in de Verenigde Staten en Duitsland. Zij verwezen naar een onderzoek van het Wetenschappelijk Onderzoeks- en Documentatiecentrum. Ook vroegen zij of effectiviteit van het tappen niet sterk zal afnemen door de introductie van encryptie.
Wij wijzen erop dat blijkens onderzoek het tappen een effectief middel is. De inzet ervan voorkomt dat de politie haar toevlucht moet nemen tot andere, meer indringende opsporingsmethoden. Het is bekend dat in bijvoorbeeld de Verenigde Staten de politie vaker moet infiltreren, met alle gevaren van dien, omdat de tapwetgeving restrictiever is dan in Nederland. Of de effectiviteit van het tappen zal afnemen door de introductie van encryptie is niet op voorhand te zeggen. Het hangt er vanaf of justitie in staat zal blijken encryptietechnieken te decoderen, en in welke mate personen die afgetapt worden gebruik maken van geavanceerde encryptietechnieken.

Deze leden vroegen om een fundamentele bezinning op de bevoegdheden van de opsporingsautoriteiten waar het gaat om digitale opsporing, nu in het digitale tijdperk een groeiend deel van het maatschappelijk leven tot stand komt met behulp van telecommunicatie-infrastructuren. Wij delen deze wens van de leden van de D66-fractie. Graag verwijzen wij naar de kabinetsnota inzake de elektronische snelweg, die wij naar verwachting aan het begin van het volgend jaar aan de Tweede Kamer zullen aanbieden.

De genoemde leden vroegen verder of verkeersgegevens, die niet onder de bescherming van artikel 13 zullen vallen, wel worden opgenomen in de opvolger van de Wet persoonsregistraties. Het antwoord is bevestigend. In de Wet bescherming persoonsgegevens staat, vanwege de technische ontwikkelingen, het concept «persoonsregistratie» niet meer centraal. Het aangrijpingspunt van deze nieuwe wet wordt het langs geautomatiseerde weg verwerken van persoonsgegevens; onder verwerken wordt ook het verzamelen en het overdragen van gegevens begrepen. Verkeersgegevens die langs geautomatiseerde weg zijn verwerkt zullen binnen dit begrip, en dus in beginsel binnen de bescherming van deze wet, vallen. Overigens zijn, onder de ontwerp-Telecommunicatiewet, aanbieders van openbare telecommunicatie in beginsel verplicht verkeersgegevens bij beëindiging van iedere oproep te vernietigen of te anonimiseren (artikel 11.5).

De leden van de D66-fractie vroegen of Internetproviders en andere aanbieders kunnen weigeren verkeersgegevens ter hand te stellen van opsporingsautoriteiten, en of abonnees van een provider kunnen eisen dat de vertrouwelijkheid van hun verkeersgegevens wordt gerespecteerd.

Abonnees van Internetproviders en andere aanbieders kunnen aanspraak maken op bescherming van hun privacy. De Internetprovider of andere dienstaanbieder is gehouden de verkeersgegevens zorgvuldig te behandelen, ook zonder dat de abonnees daar uitdrukkelijk om vragen. Dat betekent dat een dergelijke dienstaanbieder de gegevens in beginsel alleen aan Justitie zal geven wanneer er een uitdrukkelijke wettelijke plicht is. Wanneer het gaat om gegevens over telecommunicatie die heeft plaatsgevonden of zal plaatsvinden, is onder omstandigheden een last van de officier van justitie ingevolge artikel 125f Wetboek van Strafvordering voldoende. Wanneer het gaat om abonneegegevens, dient er een last van de rechter-commissaris te zijn op grond van artikel 125i Wetboek van Strafvordering. Dit is slechts anders wanneer er in een bijzonder geval sprake is van een dringende en gewichtige reden, waarbij een dergelijke last niet kan worden afgewacht (artikel 11, tweede lid, van de Wet persoonsregistraties).

De leden van de D66-fractie vroegen hoe zinvol het is om de luistervink die zich op een pas afstand van de beller ophoudt gelijk te stellen met degene die het digitale signaal onderschept of van een server haalt. De twee situaties zijn naar onze mening niet goed vergelijkbaar. Wanneer iemand een digitaal signaal onderschept of van een server haalt, zal dat, er vanuit gaande dat hij geen toestemming heeft, een inbreuk op vertrouwelijke communicatie zijn. De wetgever heeft, volgens de nieuwe tekst van artikel 13, tot taak dergelijke inbreuken te voorkomen. Als iemand ongemerkt met een beller meeluistert zonder daarvoor technische hulpmiddelen te gebruiken, is hij niet strafbaar. De artikelen 139a en 139b van het Wetboek van Strafrecht gelden alleen wanneer er een technisch hulpmiddel is gebruikt. Wij zijn ook niet voornemens deze voorwaarde voor strafbaarheid te schrappen. Van een beller mag verwacht worden dat hij zich enige inspanning, zoals het sluiten van een deur, getroost om meeluisteren te voorkomen. Wij voegen hier voor de volledigheid aan toe dat dit alles geen effect heeft op de bescherming van het telefoonverkeer over de telefoonlijn: dat de deur openstaat heeft geen invloed op het tapverbod.

De leden van de D66-fractie vroegen hoe de regering wil regelen dat nieuwkomers op de telefoonmarkt het telefoongeheim respecteren. Voor het antwoord op deze vraag verwijzen wij naar de uiteenzetting eerder in deze paragraaf.

Deze leden vroegen wat het wetsvoorstel betekent voor de aansprakelijkheid van de infrastructuurbeheerders en providers. Zullen zij aansprakelijk zijn voor de inhoud van ongecodeerde berichten, nu die niet beschermd worden, vroegen deze leden.
Anders dan deze leden veronderstellen worden ongecodeerde berichten wel door artikel 13 beschermd. De infrastructuurbeheerders en providers zijn dan ook in beginsel niet aansprakelijkheid voor de inhoud van deze berichten. Aansprakelijkheid komt eerst in beeld wanneer de boodschap voor het publiek toegankelijk is, de herkomst van de boodschap niet duidelijk is en de Internetprovider geen maatregelen treft om deze te verwijderen, hoewel hij weet van het strafbare karakter van de boodschap voor het publiek.

Deze leden informeerden of er sprake kan zijn van computervredebreuk als andere telecom- en dienstenaanbieders vertrouwelijke communicatie schenden.
Een van de middelen voor het plegen van computervredebreuk is het doorbreken van een beveiliging. De beveiliging hoeft niet een ernstige hindernis te vormen om tot de communicatie te kunnen doordringen,

voldoende is dat uit de beveiliging blijkt dat de wil van de verzender gericht is op vertrouwelijkheid. Dit is uiteengezet in paragraaf 1.1.

De leden van de D66-fractie vroegen vervolgens of de inhoud van de «inbox», «outbox» en de «trash» van een mailprogramma bij een huiszoeking doorzocht mogen worden. Zij brachten ook de positie van de Internetprovider ter sprake. Deze leden vroegen wat de regering vindt van de uitspraak van de Hoge Raad van 29 maart 1994 *(Delikt en Delinkwent,* 94 314).
Volgens de Hoge Raad zijn gegevens in het geheime geheugen van een zakcomputer die geen mededelingen inhouden, gericht tot een of meer anderen dan de gebruiker, niet aan te merken als brief in de zin van artikel 13 Grondwet. Onze benadering is geheel met die van de Hoge Raad in lijn. Artikel 13 beschermt gegevens op een computer alleen voorzover die gegevens verband houden met vertrouwelijke communicatie, en dan alleen voorzover die gegevens beveiligd zijn, bijvoorbeeld met een wachtwoord. De «inbox», «outbox» en de «trash» van een mailprogramma bevinden zich bij de zender respectievelijk de ontvanger van E-mailberichten. Wanneer de computer of het mailprogramma beschermd is met een wachtwoord, dan is de situatie vergelijkbaar met die waarbij iemand een ontvangen brief of de kopie van een verzonden brief gesloten bewaart: deze mag bij een huiszoeking niet worden geopend, tenzij daarvoor afzonderlijke toestemming is verkregen in overeenstemming met artikel 13. Dit alles laat overigens onverlet dat niet beveiligde gegevens op een computer onder omstandigheden worden beschermd door artikel 10 Grondwet en, als de computer in een woning staat, in beginsel door artikel 12. De positie van de Internetprovider is een andere: hij beheert berichten voor een derde. Hij maakt – ongeacht de vraag of de berichten ook technisch zijn beveiligd – een inbreuk op de vertrouwelijke communicatie van anderen wanneer hij de berichten aan het openbaar ministerie ter beschikking stelt, tenzij hij daar wettelijk toe verplicht is.

De leden van de GPV-fractie wezen erop dat in het tweede lid geheel in het algemeen de mogelijkheid geopend wordt bij of krachtens de wet horizontale werking toe te kennen aan het grondrecht van artikel 13. Moet dit zo ver gaan, vroegen deze leden, dat de wetgever een blanco volmacht krijgt? Kan het tweede lid zo gelezen worden dat bij of krachtens de wet regels gesteld kunnen worden met betrekking tot het communicatieverkeer tussen echtgenoten of tussen ouders en kinderen?
De wetgever beschikt nooit over een blanco volmacht, hij dient immers nieuwe wetgeving in te passen in de bestaande regelgeving en met name te bezien of niet andere grondrechten in het geding zijn. Bij het concrete voorbeeld dat deze leden geven is daar zeker sprake van: bij het communicatieverkeer tussen echtgenoten of tussen ouders en kinderen zal het recht op respect voor het familie- en gezinsleven (artikel 8 EVRM) vrijwel altijd zwaarder wegen. De wetgever zal dus alleen in zeer bijzondere gevallen regels kunnen vaststellen met betrekking tot het communicatieverkeer tussen echtgenoten of tussen ouders en kinderen. Wij kunnen daar overigens nog aan toevoegen dat elke regeling die strekt tot bescherming van vertrouwelijke communicatie en die rechten van burgers beperkt of plichten aan hen oplegt, een grondslag in de formele wet dient te hebben.[1] Het gebruik van de woorden «de wet stelt regels» heeft die strekking. Zonder wettelijke grondslag kunnen dergelijke regels dus niet tot stand komen.

4. Notificatie (derde lid, vernummerd tot vierde lid)

De leden van de PvdA-fractie vonden het vastleggen van een notificatieplicht in principe juist, maar zij vonden de uitzonderingsbepaling «indien het belang van de staat zulks dringend vordert» te ruim. Deze leden

[1] Kamerstukken II 1975/76, 13 872, nr. 3, p. 23.

vroegen waarom hier niet het advies van de Raad van State was gevolgd. Verwijzend naar de Klass-zaak en naar het advies van de Raad van State meenden zij dat een regeling waarbij na beëindiging van het afluisteren door de inlichtingen- en veiligheidsdienst notificatie zonder uitzondering achterwege dient te blijven, verder gaat dan in het belang van de staat noodzakelijk is. Met name in gevallen waarin een inbreuk op vertrouwelijke communicatie achteraf ten onrechte blijkt te zijn, achtten zij het onbillijk de schending van het recht aan de betrokkene geheim te houden. Deze leden vroegen een vergelijking te maken tussen het Britse toezicht en het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten.
Wij hebben hiervoor, in paragraaf 2.2, het Britse stelsel vergeleken met het voorgestelde Nederlandse stelsel, en toen de vraag beantwoord of het ontbreken van rechterlijk toezicht voorafgaand aan en tijdens het onderzoek geoorloofd is in het licht van artikel 8 EVRM. Onze conclusie is dat het Nederlandse stelsel tenminste aan dezelfde eisen voldoet als het Britse stelsel. De commissie van toezicht zal, zo menen wij, kunnen voorkomen dat er inbreuken worden gemaakt op het recht op vertrouwelijke communicatie die achteraf onrechtmatig blijken te zijn.
In de Klass-zaak heeft het EHRM aangegeven dat de activiteiten of het gevaar waartegen een reeks onderzoeksmaatregelen zijn gericht, nog jaren of zelfs tientallen jaren na het beëindigen van het onderzoek kan doorgaan. Notificatie achteraf kan het lange-termijndoel dat met het onderzoek wordt nagestreefd, schaden (paragraaf 58). Het Hof heeft dan ook moeten constateren dat het achterwege laten van notificatie noodzakelijk is in een democratische samenleving in het belang van de nationale veiligheid, en het voorkomen van wanordelijkheden en strafbare feiten (paragraaf 48 en 68). Het Hof vond dat aan artikel 13 EVRM is voldaan wanneer een rechtsmiddel openstaat dat zo effectief mogelijk is, gelet op de beperkte omvang van de rechtsbescherming die inherent is aan elk systeem van geheime onderzoeken (paragraaf 69). Mede gelet op de jurisprudentie van de Europese Commissie voor de Rechten van de Mens met betrekking tot het Britse stelsel van toezicht, menen wij dat het achterwege laten van notificatie noodzakelijk is in een democratische samenleving.
Wij zien echter reden om het criterium «indien het belang van de staat zulks dringend vordert» te verlaten. Zoals hiervoor (paragraaf 2.2) aangegeven wordt nu bij nota van wijziging bepaald dat beperking van het recht op vertrouwelijke communicatie slechts kan plaatsvinden op last van de rechter, of, in het belang van de nationale veiligheid, met machtiging van de minister. Met het criterium «nationale veiligheid» wordt gedoeld op de taakuitoefening door de inlichtingen- en veiligheidsdiensten. Aangezien notificatie alleen achterwege zal blijven waar het die taakuitoefening betreft, is het juister om ook het achterwege laten van notificatie te koppelen aan het begrip «nationale veiligheid». Deze aanpassing is in de nota van wijziging opgenomen.

De leden van de CDA-fractie waardeerden de kennisgevingsplicht, maar vonden het niet aanvaardbaar dat de inlichtingen- en veiligheidsdiensten geheel buiten deze plicht vallen. Zij verwezen naar het verslag inzake wetsvoorstel 25 442,[1] waarin zij, onder verwijzing naar de Klass-zaak, hebben aangegeven dat uitzonderingen op de kennisgevingsplicht slechts mogelijk zijn voor zover en voor zolang het belang van de staat zulks dringend vordert.
Zoals wij hiervoor hebben aangegeven kunnen geheime onderzoekingen onder de huidige omstandigheden noodzakelijk zijn in een democratische samenleving, in het belang van de nationale veiligheid. Notificatie kan, zo heeft het Hof aangegeven, het lange-termijndoel dat met het onderzoek wordt nagestreefd, schaden. Dat maakt het van belang om een notificatieplicht achterwege te laten.

[1] Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepalingen over het binnentreden van woningen, kamerstukken II 1997/98, 25 442, nr. 4.

De leden van de D66-fractie vroegen of het wetsvoorstel wel strookt met artikel 8 van het EVRM. Artikel 8 is, zo stelden zij, bij nauwkeurige lezing strikter dan het gehele nieuwe artikel 13.
Op de vraag of het wetsvoorstel strookt met artikel 8 EVRM is in het voorgaande ingegaan. De stelling dat artikel 8 EVRM strikter is dan het nieuwe artikel 13 Grondwet is naar onze mening te absoluut. Artikel 8 EVRM stelt, anders dan artikel 13 Grondwet, materiële normen die in acht moeten worden genomen bij het beperken van het gegarandeerde recht. Daar staat tegenover dat de reikwijdte van de term «correspondentie» in artikel 8 minder duidelijk is: het is aan de rechter om te bepalen welke vormen van communicatie eronder gerekend moeten worden. Met artikel 13 Grondwet wordt door de grondwetgever zelf een algemeen en ruim recht op vertrouwelijke communicatie gegarandeerd. Voorts verlangt artikel 13 Grondwet dat beperkingen van het recht op vertrouwelijke communicatie een formeel-wettelijke grondslag moeten hebben; de nota van wijziging voegt daar nog aan toe dat het grondrecht in beginsel alleen met toestemming van de rechter mag worden beperkt. Zulke strikte eisen liggen niet in artikel 8 EVRM besloten.

De leden van de GPV-fractie vonden het voor de hand liggen dat, bij het maken van uitzonderingen op de notificatieplicht, wordt gedacht aan de inlichtingen- en veiligheidsdiensten. Zijn er ook andere omstandigheden denkbaar waarin een beroep op het belang van de staat kan worden gedaan, zo wilden deze leden weten.
Zoals wij hiervoor aangaven hebben wij het criterium dat deze leden noemen vervangen door het criterium «in het belang van de nationale veiligheid». Met dit criterium wordt alleen gedoeld op de taakuitoefening door de inlichtingen- en veiligheidsdiensten. Voor de strafvordering is geen uitzondering op de notificatieplicht nodig.

De leden van de GPV-fractie meenden voorts dat, ook als aangenomen wordt dat het weglaten van een notificatieplicht op grond van het belang van de staat niet in strijd is met het EVRM, dit toch geen voldoende argument is om maar te kiezen voor een onbeperkte uitzondering.
Wij zijn het eens met deze leden dat aan het EVRM geen argumenten ontleend mogen worden om grondrechten in de Grondwet te beperken. Daarvan is hier echter geen sprake. De noodzaak om een uitzondering te maken op de notificatieplicht voor de inlichtingenen veiligheidsdiensten houdt echter verband met de noodzaak om de onderzoeken die deze diensten verrichten, geheim te houden. Wij hebben ons er vervolgens van moeten vergewissen of deze keuze zich verdraagt met het EVRM, zoals naar voren komt in de memorie van toelichting en vervolgens in deze nota.

Deze leden waren niet gelukkig met het doelcriterium «belang van de staat», nu dit criterium ook wordt gebruikt in artikel 68 Grondwet. Nu dit criterium is vervangen door «het belang van de nationale veiligheid», hoeft deze vraag niet meer te worden beantwoord.

De Minister-President, Minister van Algemene Zaken,
W. Kok

De Minister van Binnenlandse Zaken,
H. F. Dijkstal

De Minister van Justitie,
W. Sorgdrager