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

VOORSTEL VAN WET

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

Er bestaat grond het hierna in de artikelen II en III omschreven voorstel tot verandering in de Grondwet in overweging te nemen.

ARTIKEL II

Artikel 13 van de Grondwet komt te luiden:

Artikel 13

1. Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.
2. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, met machtiging van een of meer bij de wet aangewezen ministers.
3. De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim.

ARTIKEL III

Aan de Grondwet wordt een additioneel artikel toegevoegd, luidende:

ARTIKEL VI

Bestaande wettelijke beperkingen van het in artikel 13, eerste lid, neergelegde recht die in overeenstemming zijn met artikel 13 naar de tekst van 1983 zijn toegestaan voor ten hoogste vier jaren of tot een bij of krachtens de wet te bepalen eerder tijdstip.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren wie zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister-President, Minister van Algemene Zaken,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Veiligheid en Justitie,

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

INHOUDSOPGAVE MEMORIE VAN TOELICHTING

II. ARTIKELSGEWIJZE TOELICHTING

MEMORIE VAN TOELICHTING

I. ALGEMEEN DEEL

1. Inleiding

1.1 Algemeen

Dit wetsvoorstel strekt ertoe de reikwijdte van de onschendbaarheid van het brief-, telefoon- en telegraafgeheim dat in artikel 13 Grondwet (hierna: artikel 13) is neergelegd, uit te breiden naar alle communicatiemiddelen. In de praktijk voldoet de huidige grondwettelijke bepaling niet langer; de modernisering van artikel 13 zal moeten leiden tot een techniekonafhankelijke benadering van de reikwijdte. De directe aanleiding voor onderhavig voorstel tot wijziging van artikel 13 is gelegen in het rapport van de Staatscommissie Grondwet van november 2010 en de daaropvolgende kabinetsreactie.[1] De Staatscommissie Grondwet ging in het tweede deel van haar rapport, waarin de grondrechten centraal staan, onder meer in op het vraagstuk van grondrechten in het digitale tijdperk. Zij adviseerde een aantal grondrechten aan te passen in verband met de ontwikkelingen in de informatietechnologie. Het kabinet oordeelde in reactie op het advies van de Staatscommissie Grondwet dat de huidige techniekafhankelijke en limitatieve formulering van de beschermde communicatiemiddelen de normatieve betekenis van artikel 13 aan de wetgever en rechter in de weg staat. Zij leidt tot netelige interpretatievraagstukken en het risico van inconsistentie in de uitleg en de beoogde en gewenste rechtsbescherming. Dit probleem wordt versterkt doordat de formulering van artikel 13 ver achter loopt bij de verwante verdragsrechten waarin de laatste jaren nieuwe ontwikkelingen, normen en formuleringen zijn uitgekristalliseerd. Het onderhavige voorstel is aangekondigd in een brief[2], waarover ook is beraadslaagd in beide kamers van de Staten-Generaal.[3]

1.2 Achtergrond en noodzaak

Sinds de jaren 90 van de vorige eeuw wordt een politieke en juridische discussie over modernisering van artikel 13 Grondwet gevoerd. Deze discussie kan niet los worden gezien van de ontwikkelingen in de digitale samenleving. Informatiestromen en communicatie vinden heden ten dage hun weg via zeer diverse elektronische communicatiemiddelen. Deze digitalisering is reeds enkele decennia gaande en heeft onder meer geleid tot vergaande veranderingen in de wijze waarop communicatie in de samenleving gestalte krijgt. Maar ook nieuwe elektronische communicatiemiddelen hebben geleid tot ingrijpende wijzigingen in communicatiepatronen en informatiestromen in de samenleving. Stelden traditionele media zoals kranten, radio en tv slechts enkelen in staat te communiceren met velen en bepaalden die enkelen wat noodzakelijke en wenselijke informatie was - de nieuwe elektronische communicatiemiddelen stellen velen in staat zelf informatie te zoeken en te distribueren. Waar de oude technologie voorzag in identieke informatie voor het gehele publiek, openen de nieuwe communicatiemiddelen vele wegen voor velen om

[1] Kamerstukken II 2011/12, 31 570, nr. 20.
[2] Kamerstukken II 2011/12, 31 570, nr. 21.
[3] Handelingen I 2011/12, nr. 18, item 3, blz. 3-29; item 5, blz. 31-47 en Kamerstukken II 2011/12, 31 570, nr. 22 en nr. 23.

toegang te krijgen tot en het verspreiden van een ongelimiteerde hoeveelheid informatie. Deze digitalisering heeft de ontwikkeling van een informatiesamenleving, ook iSamenleving genoemd, verder voortgestuwd.[4] Kenmerkend voor de informatiesamenleving is onder meer dat informatie een eigenstandige economische waarde vertegenwoordigt. Het beheren, genereren, overdragen en gebruik van informatie is een wezenlijke factor van betekenis in de informatiesamenleving – ook voor de wijze waarop en de mate waarin wordt gecommuniceerd. Die veranderingen – toename van het aanbod van informatie en van het aantal communicatiemiddelen - hebben onherroepelijk gevolgen voor het communicatiegeheim dat artikel 13 beoogt te beschermen. De gedigitaliseerde informatiesamenleving stelt ons voor nieuwe vragen waar het gaat om privé, ofwel vertrouwelijk, te kunnen communiceren, met name in de gevallen waarin de tekst van het huidige artikel 13 nog niet voorziet in adequate bescherming van nieuwe communicatiemiddelen. De behoefte om privé te kunnen communiceren is in de gedigitaliseerde informatiesamenleving onverminderd groot. Artikel 13 beschermt privé-communicatie nu enkel wanneer deze plaatsvindt per brief, telefoon of telegraaf. De hoge vlucht die het gebruik van elektronische communicatiemiddelen heeft genomen in de digitale informatiesamenleving noodzaakt derhalve tot het heroverwegen van de reikwijdte van artikel 13 Grondwet.

Het huidige artikel 13 beschermt het brief-, telefoon- en telegraafgeheim. Communicatie met behulp van andere middelen worden niet door deze grondwetsbepaling beschermd. De opsomming van artikel 13 is daarmee anachronistisch: bijna niemand communiceert meer via de telegraaf, andere communicatiemiddelen hebben daarentegen een plaats verworven in de maatschappij die het belang van communicatie per brief minst genomen overtreffen. Nieuwe communicatiemiddelen en -technieken lijken enkel op gekunstelde wijze – door extensieve interpretatie – en dan nog slechts tot op zekere hoogte onder artikel 13 te brengen. In dit verband kan worden gewezen op de reden die de grondwetgever in 1983 aanvoerde om – naast het aloude briefgeheim – ook het telefoon- en telegraafgeheim constitutionele bescherming te bieden: de regering was "van mening dat naast de briefwisseling ook de communicatie door middel van telefoon en telegraaf een belangrijke plaats in het maatschappelijk verkeer heeft verworven en in verband met het privé-karakter ervan onder de grondrechten moet worden opgenomen".[5] Indien het criterium is dat communicatie privé moet zijn, ongeacht het middel of de techniek met behulp waarvan wordt gecommuniceerd, is duidelijk dat elektronische vormen van communicatie niet langer onbesproken kunnen blijven. In deze zin sluit onderhavig voorstel naadloos aan bij hetgeen de grondwetgever in 1983 voor ogen had. De mate van bescherming die artikel 13 biedt, is op dit moment afhankelijk van het gebruikte middel: communicatie per brief is op grondwettelijk niveau beter beschermd dan communicatie per telefoon. Dat doet geen recht aan één van de belangrijkste kenmerken van de digitale samenleving, te weten convergentie van communicatiemiddelen. Eén en hetzelfde communicatiemiddel wordt immers in toenemende mate gebruikt voor verschillende vormen van communicatie. Een voorbeeld is het gebruik van e-mail- en internetfuncties via mobiele telefoons, of het opvragen van audio- en videodiensten via het internet. Een verschil in bescherming louter vanwege een onderscheid van het gebruikte communicatiemiddel is dan ook niet langer gerechtvaardigd. Gelet op deze omstandigheden is modernisering van artikel 13 noodzakelijk en dringend gewenst.

Bij de voorbereiding van het onderhavige voorstel zijn naast het rapport van de Staatscommissie Grondwet 2010 ook eerdere adviezen, regeringsvoorstellen, alsmede

[4] WRR-rapport *iOverheid* (2011), p. 32 e.v.
[5] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 44.

kritiek daarop van betekenis geweest. Zo hebben wij ons rekenschap gegeven van de voorstellen die de regering in 1999 heeft ingetrokken, terwijl deze aanhangig waren in de Eerste Kamer[6], het daaropvolgende rapport van de Commissie Grondrechten in het Digitale Tijdperk (commissie-Franken)[7], de adviezen van de Raad van State naar aanleiding van de regeringsvoorstellen uit 2001[8], en kritiek vanuit de wetenschap op de eerdere voorstellen. Tot slot is vermeldenswaardig het in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties uitgebrachte rapport *Constitutional Rights and New Technologies*, een internationaal-vergelijkend onderzoek met betrekking tot grondrechten en nieuwe technologieën in België, Frankrijk, Duitsland, Zweden, Canada en de Verenigde Staten, dat in 2007 aan de Tweede Kamer is aangeboden.[9]

Een bezinning op adequate bescherming van het communicatiegeheim kan zich niet beperken tot uitsluitend de Nederlandse Grondwet. Op het internationale vlak tekent zich sinds 2000 een aantal scherpe contouren af met betrekking tot de bescherming van het communicatiegeheim in het digitale tijdperk. Op het moment dat de commissie-Franken in 2000 haar rapport uitbracht en in de eerste jaren nadien was er in internationaalrechtelijk opzicht nog weinig materiaal voorhanden met betrekking tot het vraagstuk van het brief- en telecommunicatiegeheim. Daarin is inmiddels het nodige veranderd. Mede naar aanleiding van de kritische overwegingen van de Raad van State ten aanzien van de in 2001 ingediende wetsvoorstellen[10] heeft Nederland zich vanaf 2004 in Europees verband hard gemaakt voor de totstandkoming van een richtinggevende uitspraak van de Raad van Europa. Aan een dergelijke uitspraak bestond behoefte vanwege de in sterke mate toenemende betekenis van de digitalisering en informatisering voor de Nederlandse Grondwet en voor de toekomstige visie op regelgeving van de Raad van Europa ter zake. Die inspanningen resulteerden destijds in de – op het niveau van de Raad van Europa vastgestelde - eerste *Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society* van 13 mei 2005.[11] De verklaring stelt voorop dat de grondrechten – waaronder het recht op respect voor privé-leven en correspondentie – dezelfde bescherming verdienen in een digitale omgeving als in een niet-digitale omgeving. Beperking van het respect voor correspondentie mag niet plaatsvinden vanwege het enkele feit dat de correspondentie geschiedt in een digitale vorm. Ook nadien zijn er in de Raad van Europa nog vele verklaringen en aanbevelingen tot stand gekomen met het perspectief op de naleving van mensenrechten in de digitale informatiesamenleving.[12]

Vanuit het mondiale perspectief valt wat betreft de ontwikkelingen op het mensenrechtelijk terrein na het laatste wetsvoorstel van de regering in 2001 het volgende te melden. Hiervoor werd reeds gewezen op de Verklaring van het Comité van Ministers van de Raad van Europa van 2005. Deze verklaring kwam opnieuw in mondiaal perspectief aan de orde bij gelegenheid van de *World Summit on the Information Society*, die onder auspiciën van de Verenigde Naties in november 2005 plaatsvond. In de slotverklaring van

---

[6] Kamerstukken II 1996/97, 25 443 nr. A.
[7] Rapport Grondrechten in het digitale tijdperk, Kamerstukken II 2000/01, 27 460, nr. 1, bijlage 1.
[8] Gepubliceerd in: *De grondwetsherziening 2006, Naar een nieuwe grondwet*. Documentatiereeks deel 39, SDU Uitgevers 2006, blz. 431-472 (artikel 7 Grondwet), blz. 475-495 (artikel 10 Grondwet) en blz. 499-536 (artikel 13 Grondwet).
[9] Kamerstukken II 2006/07, 27 460, nr. 5.
[10] Zie: *De grondwetsherziening 2006, Naar een nieuwe grondwet*. Documentatiereeks deel 39, SDU Uitgevers 2006, blz. 499-536 (artikel 13 Grondwet).
[11] CM (2005)56.
[12] Zie bijvoorbeeld aanbeveling CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines en aanbeveling CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet. Op 15 maart 2012 aanvaardde het Comité van Ministers van de Raad van Europa de Internet Governance Strategy 2012-2015, CM(2011)175 final

die top zijn "freedom of expression and the free flow of information" erkend als "essential" voor de informatiesamenleving. Recent nam de VN-mensenrechtenraad de Resolutie "on the promotion, protection and enjoyment of human rights on the Internet" aan, waarin de Raad stelt dat de rechten die mensen offline hebben ook online beschermd moeten worden.[13] Aldus is ook het belang van de gelding en bescherming van de grondrechten in een digitale samenleving op mondiaal niveau erkend. Wij zien hierin vanuit internationale hoek steun voor het - ook al eerder door Nederlandse kabinetten beleden - uitgangspunt dat *online* en *offline* in beginsel zoveel mogelijk dezelfde normen moeten gelden.[14] Dit adagium blijkt overigens niet altijd onverkort en eenvoudig toepasbaar. Voortschrijdend inzicht noopt tot enige nuancering van dit uitgangspunt; naarmate het ICT-recht tot verdere wasdom komt, is aandacht voor de concrete belangen die achter de rechtsnormen schuilgaan, van groot belang gebleken. Hieraan moet blijvend aandacht worden besteed. De eigenheid van de vraagstukken in de *online* wereld is immers niet altijd één op één te transponeren in de *offline* wereld.[15]

Tot slot kan betekenis van de wetgeving die in het kader van de Europese Unie tot stand is gekomen, nauwelijks worden overschat. Het EU-Handvest van de Grondrechten ziet in het algemeen op bescherming van het communicatiegeheim. De secundaire EU-wetgeving ziet tot in detail op bescherming van het elektronisch communicatiegeheim. Die ontwikkeling werd eind jaren '90 van de vorige eeuw ingezet en is al vergaand uitgekristalliseerd. Deze wetgeving heeft ook in de Nederlandse rechtsorde zijn beslag gekregen. Dit internationale juridische kader wordt nader toegelicht in paragraaf 5 van de toelichting. Daarnaast zullen in de paragrafen 2, 3 en 4, die een toelichting geven op concrete onderdelen van het onderhavige voorstel, indien relevant ook specifieke verwijzingen naar internationale verdragsbepalingen, aanbevelingen en jurisprudentie worden opgenomen.

1.3 Doelstelling

Het voorstel vervangt de onschendbaarheid van het brief-, telefoon- en telegraafgeheim door het recht op het brief- en telecommunicatiegeheim. Het heeft tot doel de huidige grondwettelijke bescherming die nu ziet op communicatie per brief, telegraaf of telefoon, uit te breiden naar alle huidige en toekomstige communicatiemiddelen. Het wetsvoorstel strekt aldus tot modernisering van het huidige artikel; met dit voorstel wordt gestreefd naar een volledig techniekonafhankelijke bescherming. Doordat niet langer enkel wordt gerefereerd aan specifieke communicatiemiddelen, maar wordt gekozen voor een specifieke (briefgeheim) en een generieke bescherming (telecommunicatiegeheim) verkrijgen ook e-mail, communicatie via de sociale media, opslag van persoonlijke bestanden in de 'cloud' en de zoekvraag om informatie op internet via een zoekmachine bescherming onder artikel 13. Het voorstel bevat een verruiming van de reikwijdte van artikel 13 tot alle telecommunicatie, ongeacht het middel of de techniek die is gebruikt om te communiceren, en brengt deze, voor zover het om de inhoud gaat, in het tweede lid onder hetzelfde niveau van bescherming als nu voor het briefgeheim geldt, namelijk dat beperking slechts mogelijk is met een voorafgaande machtiging van de rechter. Indien de beperking in het belang van de nationale veiligheid plaatsvindt, volstaat een machtiging van een bij de wet aangewezen minister. Tot slot is een algemene regelingsopdracht voor

[13] A/HRC/20/L.13 (5 juli 2012).
[14] Kamerstukken II 1999/00, 27 460, nr. 1, blz. 11
[15] *Overheden over internationalisering en ICT-recht*, C.J.C. Prins, E.J. Koops e.a., 2000, p. 85.

de wetgever opgenomen met het oog op de mogelijk veranderende betekenis van het brief- en telecommunicatiegeheim in horizontale verhoudingen en in toekomstige technologische en maatschappelijke ontwikkelingen.

1.4 Opzet van de memorie

In paragraaf 2 van deze toelichting wordt de inhoud van het brief- en telecommunicatiegeheim nader geduid, en worden de criteria om de reikwijdte te bepalen toegelicht. Ook wordt de betekenis van het brief- en telecommunicatiegeheim in horizontale verhoudingen belicht. Vervolgens komen in paragraaf 3 de gestelde voorwaarden aan beperkingen op het brief- en telecommunicatiegeheim aan de orde, te weten een wettelijke grondslag, de rechterlijke machtiging en de beperkingen in het belang van de nationale veiligheid met machtiging van een bij de wet aangewezen minister. De regelingsopdracht aan de wetgever wordt in paragraaf 4 toegelicht. Een plaatsbepaling van het voorgestelde artikel 13 tegen de achtergrond van relevante internationale regelgeving, alsook de relatie met nationale wetgeving wordt tot slot uitgewerkt in de paragrafen 5 en 6.

2. Inhoud en reikwijdte van het brief- en telecommunicatiegeheim

Het brief-, telefoon- en telegraafgeheim zoals vastgelegd in het huidige artikel 13 beschermt tegen inzage in de communicatie van staatswege. Normgeadresseerde is aldus de drager van publiek gezag of staatsmacht. Het 'brief- en telecommunicatiegeheim', dat het huidige brief-, telefoon- en telegraafgeheim zal vervangen, richt zich aldus primair tegen heimelijke inzage in de inhoud van communicatie door de overheid. Op de betekenis van dit voorstel in horizontale relaties wordt nader ingegaan in de paragrafen 2.4 en 4.1.

2.1 De inhoud van het brief- en telecommunicatiegeheim

Het rechtens te beschermen belang

Het brief- en telecommunicatiegeheim ziet op de bescherming van het belang dat een burger heeft bij privé-communicatie (of vertrouwelijke communicatie). De Staatscommissie Grondwet omschreef het belang van de bescherming van privé-communicatie als "men moet in een democratische samenleving vertrouwelijk met elkaar kunnen communiceren, zonder de angst dat de overheid meeluistert."[16] Deze invulling van het rechtens te beschermen belang, dat schuilgaat achter het huidige artikel 13, sluit in onze optiek naadloos aan bij het rechtens te beschermen belang achter het brief- en telecommunicatiegeheim in onderhavig wetsvoorstel. Met privé-communicatie wordt bedoeld communicatie die niet voor het publiek toegankelijk is, anders dan door de verzender aangewezen. Het gaat aldus om niet-openbare communicatie. Openbare communicatie wordt beschermd door het recht op vrijheid van meningsuiting dat is vastgelegd in artikel 7 van de Grondwet. Veelal wordt privé-communicatie gezien als één specifiek aspect van de persoonlijke levenssfeer dat bijzondere bescherming toekomt. De persoonlijke levenssfeer wordt beschermd door art. 10 Grondwet.[17] De privé-communicatie

[16] Rapport Staatscommissie Grondwet 2010, p. 85.
[17] Zie paragraaf 6.

wordt specifiek beschermd door artikel 13 en wordt separaat beschermd omdat de inhoud van de communicatie privé behoort te blijven. Het gaat er dus niet om dat de communicatie zich in de privé-sfeer voordoet: het communicatie*geheim* in artikel 13 beschermt een eigenstandig rechtsbelang. Burgers behoren in het kader van artikel 13 te kunnen communiceren vanuit de gedachte dat zij onbelemmerd van gedachten kunnen wisselen, gevoelens kunnen uitwisselen, informatie te kunnen vergaren of gericht informatie te kunnen verspreiden met behulp van communicatiemiddelen.

Privé-communicatie behoort volgens zowel het huidige artikel 13 als het onderhavige voorstel in het geval van gebruik van communicatiemiddelen adequaat te worden beschermd. Burgers kunnen immers alleen dan privé communiceren indien zij niet bevreesd hoeven zijn voor heimelijke inzage door derden die zijn betrokken bij de overdracht of de opslag van de inhoud van de communicatie. De kwetsbaarheid van de inhoud van de communicatie vanwege de feitelijke toegang door de derde met het beheer van de overdracht en/of opslag ervan behoort derhalve adequaat te worden ondervangen. De burger dient steeds zelf een vrijwillige keuze voor het moment waarop en de inhoud waarmee hij in de openbaarheid wil treden, te kunnen maken. Daarnaast hoort de burger zich vrijelijk en onder dezelfde omstandigheden te kunnen informeren met behulp van moderne communicatiemiddelen.

Het rechtsbelang impliceert overigens niet dat de overheid de burger onder alle omstandigheden kan en moet beschermen in zijn privé-communicatie. Voor de effectuering van de bescherming van de inhoud van de communicatie staan de gebruiker uiteenlopende communicatiemiddelen en –technieken ter beschikking, die ervoor zorgen dat hij zelf een passende bescherming van privé-communicatie kan kiezen. In horizontale rechtsrelaties speelt bijvoorbeeld het geïnformeerd beslissen, ofwel '*informed consent*', bij bijvoorbeeld de keuze voor het gebruik van bepaalde communicatiemiddelen, netwerken en diensten. Ook dienen de Wet bescherming persoonsgegevens (Wbp) en het contractenrecht in dit verband te worden vermeld. Sommige communicatiemiddelen, diensten en netwerken zijn naar hun aard immers meer geschikt dan andere om bijvoorbeeld een bericht met een uitgesproken privé-karakter over te brengen.

Het brief- en telecommunicatiegeheim

Alle vormen van telecommunicatie en de communicatie per brief verdienen naar het oordeel van de regering bescherming onder artikel 13. De brief wordt in het eerste lid separaat genoemd omdat in de verschijningsvorm van dit communicatiemiddel geen elektronische toepassing aan de orde is. Artikel 1, sub a, van de Postwet verstaat onder een brief 'de op een fysieke drager aangebrachte geadresseerde schriftelijke mededelingen'.

Telecommunicatie (samenstelling van het Griekse 'tèle' ofwel ver en het Latijnse 'communicare' ofwel mededelen) betekent strikt genomen het overbrengen van informatie over grote afstand. Met het begrip 'telecommunicatiegeheim' wordt in artikel 13 gedoeld op, anders dan intussen in de specifieke wetgeving gangbaar is, het overbrengen van informatie op afstand, ongeacht de gebruikte overdrachtsmiddelen. Het telecommunicatiegeheim in de zin van artikel 13 ziet op een uitleg die ruimer is dan het begrip telecommunicatie of het moderne synoniem daarvan, elektronische communicatie, zoals dat gebruikt wordt in bijvoorbeeld de Telecommunicatiewet, de Europese Richtlijnen of in het Verdrag van de Internationale Unie voor Telecommunicatie. In specifieke telecommunicatieregelgeving wordt onder het begrip 'telecommunicatie' enkel

'elektronische' communicatie verstaan. Het begrip biedt binnen deze specifieke regelgeving dus geen ruimte voor eventuele nieuwe, mogelijk nog te ontwikkelen (niet-elektronische) communicatiemiddelen. Dat achten wij niet opportuun met het oog op mogelijke technologische ontwikkelingen en toepassingen in de communicatietechniek in de verre toekomst. Hoewel naar de huidige stand van de wetenschap het niet waarschijnlijk is, kan immers niet worden uitgesloten dat in de toekomst ook communicatiemiddelen – anders dan elektronische – tot wasdom komen. Omwille van de bestendigheid van de bescherming van het belang bij privé-communicatie geven wij derhalve de voorkeur aan een ruimere uitleg van het begrip 'telecommunicatie' dan thans gebruikelijk is in het kader van de genoemde regelingen. Het begrip 'telecommunicatie' in de zin van artikel 13 omvat ook telecommunicatie zoals dat in de bestaande juridische kaders wordt gebruikt. Het is daarmee dus niet in tegenspraak.

Het moet voor de beoordeling of er in een concreet geval sprake is van 'telecommunicatie' wel steeds om een middel gaan dat wordt gebruikt om de informatie van a naar b te brengen. Daarbij gaat het niet uitsluitend om het *transport* (de overdracht) van informatie; telecommunicatie omvat in dit verband ook tussentijdse opslag van informatie. Zo strekt de bescherming van artikel 13 zich uit tot berichten die opgeslagen zijn in een voicemail-box van een telefonie-aanbieder of in een mailbox van een e-maildienst als Gmail.

De gedachte achter deze ruimere interpretatie van het begrip telecommunicatie is dat het voor de mate van bescherming van de inhoud van de communicatie niet moet uitmaken van welk communicatiemiddel men zich bedient. Artikel 13 is van oudsher immers gericht op het communicatiemiddel waarmee de te beschermen inhoud van de communicatie wordt overgebracht. De oorspronkelijke benadering van het communicatiemiddel wordt in dit voorstel aldus intact gelaten, maar het aantal communicatiemiddelen waarover de bescherming van artikel 13 zich uitstrekt wordt met het begrip met het begrip 'brief- en telecommunicatiegeheim' uitgebreid naar alle huidige en toekomstige communicatiemiddelen.

De inhoud van de communicatie

Communicatie betekent uitwisseling van informatie. De inhoud van de communicatie ziet in de context van het huidige artikel 13 op de gedachten en gevoelens, of informatie, die in een concreet geval op enig moment privé, dus zonder dat anderen toegang hebben tot die gedachten en gevoelens of informatie, wordt overdragen met behulp van een communicatiemiddel. Het begrip inhoud dient in dit kader ruim te worden opgevat; onder inhoud worden onder meer begrepen gevoelens, gedachten en informatie die wordt overgedragen. Dit kan onder meer via brieven, briefkaarten en tijdschriften, maar ook via e-mail, het *live*-gesprek, het telefoongesprek via Skype, informatie die wordt opgevraagd binnen een digitaal netwerk met behulp van een internetzoekmachine of middels het oproepen van informatie uit een podcast, een uitzending (informatie die wordt opgevraagd bij een omroep), het feitelijk reageren op bijvoorbeeld elektronische referenda, opiniepeilingen, enquêtes en verkiezingen. Kortom, de inhoud van brief- en telecommunicatie kan zowel tekst als beelden bevatten, maar ook muziek kan deel uitmaken van de inhoud van de communicatie. Dat is onder het huidige regime van artikel 13 niet anders, voor zover deze gevoelens, gedachten of informatie via de kanalen brief, telefoon of telegraaf worden verstuurd.

De inhoud van de communicatie wordt overigens niet onder alle omstandigheden

beschermd door het brief- en telecommunicatiegeheim. Er zijn soms immers communicatievormen aan de orde die op andere wijze – lees elders - grondwettelijke bescherming verkrijgen. In paragraaf 2.2 zullen de criteria worden uitgewerkt die bepalen of en in welke mate de inhoud van de communicatie bescherming van artikel 13 toekomt, en voor zover dat niet het geval is, op welke wijze de inhoud van de communicatie dan wel bescherming verkrijgt.

De inhoud van de communicatie is te onderscheiden van de gegevens die worden gegenereerd met betrekking tot de totstandkoming, de duur en het tijdstip van de communicatie. Deze gegevens worden hierna geduid als verkeersgegevens (in overeenstemming met EU-regelgeving). De adressering, het tijdstip van verzending en de duur van de overdracht of de opslag van een bericht zijn voorbeelden van dit type gegevens. De verkeersgegevens worden op dit moment beschermd door art. 10 Grondwet, het algemene recht op eerbiediging van de persoonlijke levenssfeer. Deze gegevens behoren niet primair tot het belang dat artikel 13 beoogt te beschermen, omdat zij niet de inhoud van het bericht weergeven. Niet kan worden uitgesloten dat zij daarvan wel deel uitmaken indien zij nauw verband houden met de inhoud van het bericht. De verkeersgegevens gegevens worden nader besproken in paragraaf 2.3.

2.2 De reikwijdte van het brief- en telecommunicatiegeheim

De reikwijdte van het brief- en telecommunicatiegeheim dient voor zijn toepassing nader te worden bepaald. Om te kunnen bepalen of het brief- en telecommunicatiegeheim in een concrete situatie aan de orde zijn, worden drie cumulatieve criteria gehanteerd, te weten het gebruik van een communicatiemiddel in het communicatieproces, de aanwezigheid van een derde die is belast met het beheer over de overdracht en/of opslag van de communicatie en tot slot de noodzaak van de gerichtheid van de communicatie. Deze drie criteria worden hierna verder uitgewerkt.

Aanwezigheid van communicatiemiddelen

In het licht van de visie op het belang bij privé-communicatie en de voorgenomen modernisering van artikel 13 hebben wij ons opnieuw beraden op de vraag op welke wijze dit belang het meest adequaat kan worden beschermd. Zoals destijds door de Commissie-Franken en ook door de Staatscommissie Grondwet is onderkend, belichaamt artikel 13 van de Grondwet van oudsher het recht om zonder dat derden kennis kunnen nemen van de inhoud van een bericht, gebruik te maken van bestaande en met name genoemde communicatiemiddelen. Het gaat er aldus primair om dat de burger erop kan vertrouwen dat de inhoud van een bericht dat ter verzending en bezorging op de geadresseerde plaats aan de zorg van een derde is toevertrouwd ook daadwerkelijk wordt verzonden en bezorgd zonder dat een derde – ongeautoriseerd - kennis neemt van de inhoud ervan. De gerichtheid op het communicatiemiddel blijkt duidelijk uit de tekst van de vroegere grondwetsbepalingen van het huidige artikel 13. Die spraken sinds 1840 over "het geheim der aan de post of andere openbare instelling van vervoer toevertrouwde brieven".[18] Deze zinsnede is in 1983 geschrapt om te bereiken dat het briefgeheim zich ook zou uitstrekken tot andere overheidsinstellingen. Het kabinet heeft zich destijds niet expliciet uitgesproken

[18] Zie ook B.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002*, Deventer 2002, p. 24-27 en 51 en E.J. Dommering (red.), *Informatierecht*, Amsterdam 2000, p. 71.

over de vraag of de regeling ook geldt voor gevangenisdirecties in verband met de bepaling van artikel 15, vierde lid, van de Grondwet.[19] In die gevallen gaat het eveneens het om de eerbiediging van "het geheim van een aan hen ter aflevering aan een derde toevertrouwde brief".[20] Ook het huidige artikel 13 richt zich - ongeacht het communicatiemiddel dat wordt gebruikt - primair op de bescherming van de inhoud van communicatie tegen inzage door anderen, inclusief degenen die het communicatiemiddel beheren.[21]

Wij menen op grond van het voorgaande dat het brief- en telecommunicatiegeheim zich primair dient te richten op een door een derde beheerd communicatiemiddel. Dat komt volgens ons tot uitdrukking in de woorden "het recht op bescherming van het brief- en telecommunicatiegeheim". Achter zowel de aanduiding "brief" als het begrip "telecommunicatie" gaat immers het specifiek respectievelijk generiek aangeduide communicatiemiddel schuil door middel waarvan de overdracht van de communicatie tot stand wordt gebracht.

Welke de aard is van het communicatiemiddel doet dan niet ter zake: zodra sprake is van communicatie met behulp van een door een derde beheerd communicatiemiddel is het brief- en telecommunicatiegeheim aan de orde. Het privé-karakter van de inhoud van de communicatie behoeft aldus niet als zodanig te worden aangetoond voor bescherming van artikel 13. Zou dat wel het onderscheidende criterium zijn, dan zou de ongewenste situatie kunnen ontstaan dat niet als zodanig bedoelde communicatie tijdens het transport in principe geen bescherming behoeft, en dat de derde met het beheer over de overdracht en de eventuele bewaring zelf kan gaan differentiëren tussen privé-communicatie en niet als zodanig bedoelde communicatie.

De derde met het beheer over de overdracht en/of opslag

Men moet erop kunnen vertrouwen dat aan een derde toevertrouwde communicatie ter bestemde plaatse wordt bezorgd zonder dat anderen kennis kunnen nemen van de inhoud ervan - tenzij uit de wijze van de communicatie onmiskenbaar volgt dat die beslotenheid niet beoogd is (zoals bij een toespraak of een publicatie op het internet). Dit impliceert dat de bescherming beperkt blijft voor zover en zolang de inhoud van communicatie aan een derde voor de overdracht en/of opslag is toevertrouwd. Voorheen werd de duur van de bescherming bepaald door de zogenoemde 'transportfase', die in het fysieke communicatieproces nog helder af te bakenen was van een ontwerpbericht en ontvangst van het bericht na transport. Zodra de brief door de postbode werd afgeleverd en de betreffende brief op de deurmat viel, hield de betrokkenheid van de derde in het communicatieproces op en mitsdien ook de bescherming van artikel 13. Bij gebruikmaking van elektronische communicatiemiddelen versmelt de 'transportfase' veelal met het moment van de opslag van het bericht in de conceptfase en bewaring van het bericht na afloop van het transport, omdat op die momenten de derde ook al of nog steeds het beheer heeft over het bericht. De derde beheert in dergelijke gevallen vaak ook de opslag van het bericht. Veelal is deze derde in deze situatie dan feitelijk in de gelegenheid kennis te nemen van de inhoud van het bericht. De vraag rijst in het kader van het brief- en telecommunicatiegeheim of de overheid in de situatie van de overdracht of de opslag van

[19] Bax 2005, p. 113. Het EVRM bood gedetineerden echter ook de bescherming van het briefgeheim. Zie onder meer *Golder t. Verenigd Koninkrijk*, EHRM 21 februari 1975, series A 18 en *Silver t. Verenigd Koninkrijk*, 25 maart 1983 series A 61.
[20] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 44.
[21] Zie ook HR 18 oktober 1994, NJ 1995, 101.

het bericht kennis mag nemen van berichten - wanneer ze nog in concept in bijvoorbeeld de persoonlijke Google-*inbox* zijn opgeslagen (het bericht bevindt zich in het beheer van Google), of wanneer het bericht is gelezen en opgeslagen blijft in de *inbox* van de ontvanger (het bericht bevindt zich in het beheer van de dienstverlener die de ontvanger heeft aangewezen voor ontvangst en bewaring van berichten). Is het toegestaan dat de overheid kennis neemt van een bericht dat is verzonden naar de *inbox* van een beperkt aantal 'vrienden' in bijvoorbeeld Facebook?

De technologische werkelijkheid, waarin opslag en overdracht van het bericht als het ware met elkaar versmelten, dient te worden vertaald in de reikwijdte van het brief- en telecommunicatiegeheim omdat de bescherming heeft te gelden zolang de derde feitelijk toegang tot de inhoud van het bericht heeft. Onder deze omstandigheden is het belang van de verzender bij privé-communicatie immers kwetsbaar. Maatgevend is dat zolang de derde het bericht beheert en toegang heeft tot de inhoud, de bescherming van het brief- en telecommunicatiegeheim dient te gelden. Dat betekent dat de bescherming van artikel 13 bijvoorbeeld geldt in de zojuist genoemde situaties – opslag van een conceptbericht, opslag in de *inbox* na ontvangst en na lezing door de ontvanger en berichtenverkeer op één van de sociale media - en dat de overheid noch via de derde noch direct bij de verzender kennis mag nemen van de inhoud van het bericht zonder dat daarvoor een formeelwettelijke grondslag bestaat en er een rechterlijke machtiging is gegeven.

In het leeuwendeel van de gevallen is de derde die de overdracht en eventueel opslag verzorgt echter niet de overheid, maar een private partij. Ook de derde in de hoedanigheid van private partij die de overdracht en eventueel opslag verzorgt, mag niet zonder toestemming van de verzender kennisnemen van het bericht. Deze bescherming is verankerd in de uitvoeringswetgeving die onder meer is gebaseerd op het belang van privé-communicatie dat artikel 13 Grondwet beoogt te beschermen (zie artikel 4 Postwet 2009 en artikel 18.13 Telecommunicatiewet). Op de werking van het brief- en communicatiegeheim in horizontale verhoudingen wordt in paragraaf 2.4 nader ingegaan.

Uitgaand van het vereiste van de aanwezigheid van een communicatiemiddel en de derde die de overdracht van de inhoud van het bericht voor zijn rekening neemt, betekent dat inderdaad – zoals de Raad van State in zijn advies van 2002 opmerkte – dat artikel 13 wel in de weg staat aan een telefoontap, maar niet aan het afluisteren van een telefoongesprek door middel van een vlak naast één van de sprekers geplaatste microfoon. Het *live-gesprek* in de openbare ruimte wordt vanwege het feit dat een derde niet betrokken is bij de overdracht van de inhoud van de communicatie, niet beschermd. Het *live-gesprek* is echter niet onbeschermd. Vindt het live-gesprek plaats in de openbare ruimte, dan is bescherming van art. 10 Grondwet aangewezen. Indien het wordt gevoerd in huiselijke sfeer geldt tevens de bescherming van artikel 12 Grondwet dat ziet op de onschendbaarheid van de woning. Bij het *live-gesprek* gaat het om een ander type kwetsbaarheid dan bij het brief- en telecommunicatiegeheim. Bij het *live-gesprek* speelt heimelijkheid van de observatie, die bij de onschendbaarheid van de woning en bij de lichamelijke integriteit ook aan de orde is. Bij het brief- en telecommunicatiegeheim wordt de inhoud van de communicatie aan een derde toevertrouwd, waarmee de controle over het bericht uit handen wordt gegeven. Omgekeerd betekent het voorgaande dat de bescherming van het brief- en telecommunicatiegeheim aan de orde is zolang de communicatie in de feitelijke beschikkingsmacht van de derde is, dat wil zeggen zolang deze derde het beheer heeft over de overdracht en/of opslag van de inhoud van het bericht. Daaraan doet niet af dat wellicht op enig moment ook de geadresseerde toegang tot die communicatie kan krijgen – de Raad van State wees hier op de postbus op het postkantoor, een poste-restante-stuk, een e-mail in de berichtenbox en een

voicemailbericht. Het gaat immers om bescherming van aan derden toevertrouwde communicatie tegen inmenging door een overheidsfunctionaris; zolang de derde het beheer heeft over de communicatie is dat risico aanwezig en is bescherming aangewezen.

Gerichtheid van de communicatie

Het brief- en telecommunicatiegeheim beschermt gerichte communicatie, dat wil zeggen communicatie die (uitsluitend) is gericht aan één of meer specifieke ontvangers. In het communicatieverkeer is steeds vast te stellen of communicatie gericht is, hetgeen dit criterium een noodzakelijke en bruikbare mate van objectiveerbaarheid verleent. Niet alleen de brief, de e-mail of het bericht dat via een *sociaal medium* aan een aantal ontvangers (zoals Facebook) wordt verstuurd, valt onder de reikwijdte van artikel 13, maar ook gerichte reclame-uitingen, het oproepen van informatie uit een digitaal netwerk (een zoekmachine, Wikipedia, Youtube of een programma van een omroep) en *spam*. De communicatie moet met andere woorden, wil de verzender bescherming van artikel 13 genieten, gericht zijn. Gerichte communicatie houdt in dat het bericht van de verzender wordt verstuurd aan een of meerdere afzonderlijk te bepalen geadresseerden. Denkbaar is dat de verzender iets aan zichzelf adresseert, bijvoorbeeld door zichzelf te mailen (al dan niet naar een ander e-mailadres), of bij opslag van communicatie in de *cloud*. Ongerichte communicatie kenmerkt zich daarentegen door de wens tot vrije meningsuiting en wordt beschermd door artikel 7 van de Grondwet. Dan gaat het bijvoorbeeld om een *realtime* radio- of tv-uitzending of een podcast – in de genoemde gevallen is geen sprake van afzonderlijke te bepalen adressen.

De eis van gerichtheid van de communicatie is onder het huidige artikel 13 niet anders.[22] Het begrip 'gerichtheid' moet in dit verband ruim worden opgevat. Het kan gaan om het gericht zijn van de communicatie aan natuurlijke personen maar ook om berichten aan - èn van - organisaties, instellingen en andere entiteiten. Rechtspersoonlijkheid in civielrechtelijke zin is niet vereist. Evenmin is vereist dat de 'persoon' of 'entiteit' die communiceert of met wie wordt gecommuniceerd feitelijk zelf betrokken is bij de communicatie: ook een automatisch gegenereerde ontvangstbevestiging per brief, een afwezigheidsbericht per e-mail, het versturen van een formulier via een website of het opvragen van informatie bij een geautomatiseerde beldienst of internetdienst worden vanwege hun gerichtheid beschermd door artikel 13. Het persoonlijke kan blijken uit uiteenlopende soorten adresseringen: postadres, telefoonnummer, *Internet Protocol*-adres of welke vorm van adressering ook. Het achterlaten van een boodschap op een voor iedereen toegankelijke website, zoals bijvoorbeeld het achterlaten van een bericht op Twitter kan evenwel niet als gerichte communicatie worden gezien. De inhoud van een bepaalde voorstelling, een openbare toespraak, informatie op het internet of *realtime audio en -video* zoals een *live*-radiouitzending of televisie zijn in beginsel ook geen gerichte communicatie. In die gevallen is veeleer sprake van situaties waarop de uitingsvrijheid van toepassing is, zoals het openbaren van een gedachte – vergelijkbaar met het langs de openbare weg aanplakken van een pamflet – hetgeen uitsluitend valt onder het toepassingsbereik van artikel 7 van de Grondwet. In zoverre komt dus ook in het thans voorgestelde artikel 13 nog enige betekenis toe aan de wijze waarop de verzender zijn boodschap verstuurt: communicatie wordt beschermd, tenzij uit de wijze waarop de communicatie plaatsvindt onmiskenbaar blijkt dat de verzender zijn boodschap

[22] Van der Pot/Donner, p. 73 en HR 29 maart 1994, D&D 1994, p. 314.

in de openbaarheid wil brengen. In dat laatste geval is geen sprake van gerichte communicatie in de door ons bedoelde zin.

Twee voorbeelden kunnen de door ons gekozen gerichtheid als criterium verduidelijken. Geen bescherming bestaat voor het *chatten* in voor iedereen toegankelijke discussiegroepen. Wordt echter *gechat* in een besloten groep, dan is bescherming van artikel 13 ten volle aan de orde. Evenmin is bescherming aan de orde wanneer een omroepdienst een uitzending verzorgt; die communicatie wordt geacht te zijn beschermd door de vrijheid van meningsuiting onder artikel 7 Grondwet omdat deze ongericht is. Indien een individu een omroepdienst benadert met de vraag om een specifieke uitzending die vervolgens via het *video-on-demand*-principe wordt verstuurd aan de verzoeker, ontstaat de situatie waarin bescherming van artikel 13 wel aan de orde is.[23] De gerichtheid van de communicatie is aldus een aanvullend criterium voor de toepasselijkheid van artikel 13. Deze nadere invulling van het brief- en telecommunicatiegeheim als bescherming van het communicatiemiddel is noodzakelijk, nu communicatiemiddelen in toenemende mate worden benut voor zowel besloten, gerichte communicatie als openbare, ongerichte communicatie. Het voorbeeld van de omroep illustreert dit. Dit wisselende gebruik van communicatietechnieken voor zowel massacommunicatie als besloten communicatie wordt ook wel aangeduid met het begrip "convergentie".[24] Genoemde afbakening van het brief- en telecommunicatiegeheim is noodzakelijk om te voorkomen dat het toepassingsbereik ervan onverantwoord ruim wordt. Wanneer iemand tegelijk aan vele mensen een e-mail of SMS-bericht verstuurt, is eveneens sprake van gerichte communicatie: de geadresseerden – hoezeer ook velen in getal – zijn immers nog altijd individueel herleidbaar. Het aantal specifiek geadresseerden vormt geen onderscheidend criterium. Onder het huidige artikel 13 wordt bijvoorbeeld ook reeds een gelijktijdig aan alle leden van een vereniging verzonden nieuwsbrief door het grondrecht beschermd. De inhoud van ongerichte communicatie valt aldus buiten het bereik van artikel 13. Tot ongerichte communicatie horen bijvoorbeeld de toespraak, omroep en radio met *realtime*-uitzendingen (al of niet via de ether of internet), het internet, of een voorstelling. De inhoud, of de informatie die in ongerichte communicatie wordt verspreid, valt samen met het recht op vrijheid van meningsuiting en het achterliggend rechtsbelang bij communicatievrijheid dat artikel 7 Grondwet beoogt te borgen.[25]

Samenvattend kan worden vastgesteld dat er drie cumulatieve criteria zijn die tezamen de reikwijdte van het brief- en telecommunicatiegeheim bepalen. Artikel 13 is van toepassing indien gebruik wordt gemaakt van een communicatiemiddel, indien een derde is betrokken die de communicatie beheert en aldus toegang heeft tot de inhoud, en indien sprake is van gerichte communicatie. De inhoud van het bericht wordt dan steeds door het brief- en telecommunicatiegeheim beschermd, ongeacht of de verzender van het bericht dit nu zo bedoeld heeft of niet.

2.3 Verkeersgegevens

Bij communicatie met gebruikmaking van daartoe bestemde kanalen ontstaan gegevens die niet zien op de gecommuniceerde boodschap als zodanig, maar die betrekking hebben op de overdracht of op de opslag van het bericht. Te denken valt bijvoorbeeld aan

[23] Deze benadering sluit aan bij de ePrivacyrichtlijn van de Europese Unie, zie hierna par. 5.1.
[24] Hierover in verband met de situatie in Duitsland Thomas Hoeren and Anselm Rodenhausen, Constitutional Rights and New Technologies in Germany, in: B.J. Koops e.a. (red.), *Constitutional Rights and New Technologies*, Tilburg 2007, p. 103 en 104.
[25] De verhouding tussen art. 7 en artikel 13 wordt besproken in paragraaf 6.1.

gegevens over tijdstip, plaats, duur van en betrokken nummers bij een telefoongesprek en gegevens over tijdstip, adressering en omvang van een e-mailbericht. Zij zien niet op de inhoud van de communicatie en worden hierna aangeduid als 'verkeersgegevens'.

Opgemerkt zij dat de juridische definitie van verkeersgegevens op de diverse rechtsterreinen op verschillende wijzen wordt vastgesteld. Artikel 126n Wetboek van Strafvordering omschrijft deze gegevens als (bij algemene maatregel van bestuur aangewezen) "gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker". Dergelijke gegevens, die thans in het Besluit vorderen gegevens telecommunicatie zijn aangewezen als verkeersgegevens, hebben geen betrekking op de inhoud van telecommunicatie en vallen derhalve niet onder de werking van artikel 13. Verkeersgegevens kennen in de EU-Richtlijnen die zien op elektronische communicatienetwerken en -diensten een eigen, reeds vastgelegde betekenis.[26] In deze betekenis omvatten verkeersgegevens die gegevens, die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan. Verkeersgegevens worden ook wel "inhoudloze transmissiegegevens" genoemd.[27] Voor zover verkeersgegevens tevens persoonsgegevens zijn, worden deze beschermd door artikel 10 Grondwet. Bezien vanuit het hiervoor beschreven rechtens te beschermen belang vallen verkeersgegevens, omdat het geen inhoud van de communicatie betreft, buiten de reikwijdte van artikel 13.

Verkeersgegevens geven op zich geen inzicht in de inhoud van de communicatie, maar wel in andere aspecten die verband kunnen houden met de inhoud van de communicatie.[28] Verkeersgegevens kunnen bovendien naar hun aard raken aan de telecommunicatievrijheid. Met instemming wordt op dit punt verwezen naar de opmerking van de Raad van State ter zake van metagegevens in zijn advies op het wetsvoorstel uit 2001: "De strekking van artikel 13 is dat burgers zonder inmenging vertrouwelijk met elkaar kunnen communiceren. Zou iemand weten of vermoeden dat de overheid weet welke telefoongesprekken hij voert, dan zou dat voor hem reden kunnen zijn om bepaalde gesprekken niet meer te voeren. Dit doorbreekt de vertrouwelijkheid van de communicatie op zichzelf niet, maar raakt wel de vrijheid van (tele)communicatie."[29] De Commissie Franken en de meerderheid van de Staatscommissie Grondwet wilden verkeersgegevns niet binnen de reikwijdte van artikel 13 brengen.[30]

In dit wetsvoorstel is het standpunt van de beide commissies gevolgd en zijn verkeersgegevens niet onder de reikwijdte van artikel 13 gebracht. De reden daarvan is dat zij niet de inhoud van de telecommunicatie betreffen en dat een andersluidende keuze tot gevolg zou hebben dat voor inzage in verkeersgegevens steeds een rechterlijke machtiging nodig zou zijn, hetgeen gelet op de aard van deze gegevens te vergaand zou zijn.

Aandacht verdient evenwel dat de inhoud van telecommunicatie in technische zin

---

[26] Art. 5, eerste lid, van de ePrivacyrichtlijn luidt: 'Tot verkeersgegevens behoren onder meer gegevens met betrekking tot de routering, de duur, het tijdstip of het volume van een communicatie, het gebruikte protocol, de locatie van de eindapparatuur van de verzender of de ontvanger, het netwerk waarop de communicatie begint of eindigt en het begin, het einde of de duur van de verbinding'. Er is geen sprake van een gesloten lijst van gegevens die hiertoe behoren.
[27] A.H.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen 2006, p. 4 en 5.
[28] L.F. Asscher en A.H. Ekker, *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam 2003.
[29] W01.01.0467/I, p. 6 en 7. In dezelfde zin de Registratiekamer (voorganger van het College Bescherming Persoonsgegevens) in zijn reactie op het rapport van de commissie-Franken: (vindplaats).
[30] Rapport Staatscommissie Grondwet, p. 89. De minderheid wenste verkeersgegevens wel onder de reikwijdte van artikel 13 te brengen, zie p. 88 van het rapport.

soms ook als een verkeersgegeven wordt gezien. Zo wordt het onderwerp van een e-mail in technische zin wel tot de verkeersgegevens betreffende die e-mail gerekend. Maar in juridische zin valt het onderwerp van een e-mail onder de reikwijdte van artikel 13 omdat dat onderwerp betrekking heeft op de inhoud van de e-mail. Een ander voorbeeld is een sms-bericht: technisch gezien is een dergelijk bericht in zijn geheel een verkeersgegeven, maar juridisch gezien omvat een sms-bericht – naast verkeersgegevens – tevens de inhoud van communicatie. De conclusie is dat aan de bescherming van artikel 13 niet kan afdoen dat gegevens die de inhoud van de telecommunicatie betreffen in technische zin als een verkeersgegeven worden beschouwd. Verkeersgegevens die niet mede betrekking hebben op de inhoud van telecommunicatie vallen echter buiten de reikwijdte van artikel 13.

2.4 Horizontale werking

Grondrechten richten zich in essentie op de verhouding tussen overheid en burger, maar dat betekent geenszins dat aan de daarachter schuilgaande rechtsbelangen in horizontale verhoudingen geen betekenis toekomen.[31] Dit is ook reeds erkend door de grondwetgever van 1983. Ook in het licht van artikel 13 staat de bescherming van de burger tegen inbreuken van de overheid voorop, met name in het licht van optreden van politie en inlichtingendiensten. Anders dan in het verleden is echter op veel terreinen die verband houden met het grondrecht van artikel 13 de rol van de overheid geminimaliseerd of heeft deze zelfs nooit bestaan. Dat geldt in de eerste plaats voor de diensten van post en telefonie: die diensten worden thans uitsluitend geleverd door private partijen. Communicatie via internet en e-mail is nooit in handen van de overheid geweest.

Eén en ander benadrukt het belang van voorzieningen gericht op bescherming van het communicatiegeheim in private verhoudingen. Zoveel is immers duidelijk: het inperken van de overheidsmacht op dit punt volstaat niet. Zowel het rapport van de Commissie-Franken als het wetsvoorstel van het toenmalige kabinet bevatten destijds een voorziening in dit verband in de vorm van een artikellid waarin de gewone wetgever de opdracht kreeg regels te stellen "ter bescherming van de vertrouwelijkheid van de communicatie". De Staatscommissie Grondwet wijdde evenwel geen beschouwing aan een dergelijke regelingsopdracht.

Volgens het toenmalige kabinet was een verdergaande regeling van de horizontale werking binnen het kader van hoofdstuk 1 van de Grondwet niet goed denkbaar. Bij deze opvatting wordt thans aangesloten. De toegevoegde waarde van een bepaling als hier bedoeld moet vooral worden gezien in het feit dat hiermee de bescherming van het brief- en telecommunicatiegeheim in private verhoudingen tot zorg van de overheid wordt verklaard. Wij kunnen ons vinden in deze overwegingen, en wijken daarmee af van de Staatscommissie Grondwet. Wij voegen daaraan echter het volgende toe. Zoals eerder in deze memorie is opgemerkt, behelst het onderhavige voorstel een modernisering van artikel 13. Daarmee bedoelen wij dat de huidige voorstellen geen bepalingen bevatten die niet passen binnen de huidige systematiek van hoofdstuk 1 van de Grondwet. Een bepaling inzake de horizontale werking van artikel 13 kan in dat licht enkel worden geformuleerd in de vorm van een regelingsopdracht aan de formele wetgever. Daarop wordt in paragraaf 4.1. dieper ingegaan.

---

[31] L.F.M. Verhey, *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy*, diss. UU 1992.

3. Beperkingen

3.1 Algemeen

De grondwettelijke bescherming van het brief- en telecommunicatiegeheim is niet absoluut. Er kunnen redenen van algemeen belang zijn die een beperking rechtvaardigen, zoals het voorkomen, de opsporing en de vervolging van strafbare feiten of in het belang van de nationale veiligheid. De huidige grondwetsbepaling maakt onderscheid tussen de beperkingen die zijn toegestaan op het briefgeheim, namelijk in de gevallen bij de wet bepaald op last van de rechter en de beperkingen die zijn toegestaan op het telefoon- en telegraafgeheim, namelijk in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Breed gedeeld is de opvatting dat dit onderscheid in beschermingsniveau als gevolg van technologische ontwikkelingen niet langer houdbaar, noch wenselijk is. De bescherming hangt dan te zeer af van de interpretatie van de reikwijdte van een bepaald communicatiemiddel, terwijl met e-mail, sms en internettoegang via een mobiele telefoon het onderscheid tussen enerzijds de brief en anderzijds de telefoon, telegraaf en nieuwe communicatiemiddelen die in dit voorstel onder de reikwijdte van artikel 13 komen te vallen, vervaagt. De regering ziet bovendien geen objectieve rechtvaardiging voor dat verschil in rechtsgevolg. Voor zover de maatschappelijke betekenis van bepaalde communicatiemiddelen een zinvol criterium kan zijn, wordt opgemerkt dat de klassieke brief eerder aan betekenis heeft verloren ten opzichte van moderne communicatiemiddelen. Ook de Commissie-Franken stelde al dat het verschil in beperkingsgronden niet gerechtvaardigd wordt door een verschil in appreciatie van de aard of de betekenis van de verschillende communicatiemiddelen, maar uitsluitend valt te verklaren met een verwijzing naar de (wets)geschiedenis. Het parlement achtte het in het kader van de grondwetsherziening 1983 niet juist om afstand te doen van het sinds 1848 geldende vereiste van de rechterlijke last voor het briefgeheim, omdat dit zou kunnen worden uitgelegd als een achteruitgang van het beschermingsniveau.[32] Tot slot past het onderscheidenlijk behandelen van communicatiemiddelen in de Grondwet niet bij het doel van dit wetsvoorstel: het techniekonafhankelijk maken van artikel 13. In dit wetsvoorstel kiezen wij dan ook voor één regime van beperkingsmogelijkheden van het brief- en telecommunicatiegeheim, zonder onderscheid tussen de gebruikte communicatiemiddelen, in combinatie met een ander regime voor beperkingen in het belang van de nationale veiligheid, waarop nader zal worden ingegaan in paragraaf 3.3. Dit betekent dat het onderscheid tussen toegestane beperkingen op het brief- en telecommunicatiegeheim niet langer middelgebonden, maar doelgebonden is.

De algemene eis die het voorgestelde artikel 13 stelt, is dat de formele wetgever bepaalt in welke gevallen beperkingen zijn toegestaan. Delegatie is niet toegestaan. Wij delen verder de opvatting van de staatscommissie Grondwet en van het toenmalige kabinet dat er aanleiding bestaat een rechterlijke machtiging te introduceren als algemeen beperkingsvereiste voor inbreuken op het communicatiegeheim, dus ongeacht de voor de communicatie gebruikte techniek.[33] Daarmee wordt het beschermingsniveau van artikel 13 in algemene zin verhoogd: in beginsel volstaat niet langer machtiging van een door de wet aangewezen functionaris voor inbreuk op een telefoongesprek – voortaan is ook daarvoor

[32] Rapport Commissie-Franken, p. 150, 156 en Kamerstukken II 2000/01, 27 460, nr. 1, blz. 27-28.
[33] Rapport Staatscommissie Grondwet, p. 87; Kamerstukken II 2000/01, 27 460, nr. 1, blz. 27-28 en het niet ingediende regeringsvoorstel gepubliceerd in De grondwetsherziening 2006 Eerste lezing, tweede gedeelte, Naar een nieuwe grondwet. Documentatiereeks deel 39, blz. 510-511 (blz. 10-11 van de memorie van toelichting).

een rechterlijke machtiging vereist. Delegatie is niet toegestaan. Ook delen wij de opvatting en de daarvoor aangevoerde redenen van de commissie-Franken en het toenmalige kabinet dat een algemene uitzondering op genoemd uitgangspunt gewenst is voor zover de beperking van het brief- en telecommunicatiegeheim plaatsvindt in het belang van de nationale veiligheid. In het belang van de nationale veiligheid zijn beperkingen toegestaan met machtiging van een of meer daartoe bij de wet aangewezen ministers. Deze keuzes worden nader toegelicht in de paragrafen 3.2 en 3.3.

Overwogen is om voor beperkingen op het brief- en telecommunicatiegeheim op het niveau van de Grondwet alleen een formeelwettelijke grondslag te eisen en nadere regulering over te laten aan de gewone wetgever. Voor een dergelijk competentievoorschrift heeft de grondwetgever gekozen in artikel 10, eerste lid (eerbiediging van de persoonlijke levenssfeer) en artikel 12 van de Grondwet (huisrecht). Daarmee zou het concrete niveau van bescherming feitelijk worden overgelaten aan de gewone wetgever, die daarbij indien gewenst wel onderscheid zou kunnen maken tussen verschillende communicatiemiddelen. Een dergelijk voorstel werd in 2001 ten aanzien van artikel 13 Grondwet bepleit door de Commissie strafvorderlijke gegevensvergaring in de informatiemaatschappij (commissie-Mevis). De commissie-Mevis vroeg zich af of het grondwettelijke procedurevoorschrift van een rechterlijke last niet een te star voorschrift zou blijken te zijn gelet op de ontwikkeling van communicatietechnieken.[34] De aard van de inbreuk zou wellicht verschillen naar gelang de gehanteerde techniek. De commissie-Mevis waarschuwde in reactie op het voorstel van de commissie-Franken in het bijzonder voor het eisen van een rechterlijke machtiging voor inzage van verkeersgegevens. In ons voorstel zullen verkeersgegevens in beginsel bescherming van artikel 10 genieten, dat beperkingen op de eerbiediging van de persoonlijke levenssfeer bij of krachtens de wet toestaat. Het is echter niet ondenkbaar dat er situaties zijn waarin bescherming door artikel 13 aan de orde is. Zoals hiervoor opgemerkt zal de afbakening ter zake zich in de rechtspraktijk kunnen ontwikkelen.

In het verleden is van diverse zijden betoogd dat het aanwijzen van de tot beperking bevoegde autoriteit volledig aan de formele wetgever zou moeten worden overgelaten.[35] Wij menen echter dat voor een inbreuk op het brief- en telecommunicatiegeheim een extra waarborg in de vorm van een rechterlijke toetsing gerechtvaardigd blijft. Dit uitgangspunt spoort ook met jurisprudentie van het Europese Hof voor de Rechten van de Mens, waaruit kan worden afgeleid dat rechterlijke toetsing voorafgaand aan inzage in de inhoud van de brief- en telecommunicatie hoewel geen absolute eis, in beginsel wenselijk is omdat inzage heimelijk plaatsvindt en de betrokkene hiervan vrijwel nooit weet heeft.[36] Het stellen van de eis van een rechterlijke machtiging in de Grondwet geeft een sterke en duidelijke rechtsstatelijke waarborg. Ook in eerdere voorstellen koos de regering er uiteindelijk voor om de eis van een rechterlijke machtiging in de Grondwet zelf op te nemen.[37] Zowel de Raad van State als diverse Kamerfracties drongen daar destijds nadrukkelijk op aan bij het kabinet.

Wat betreft de onderlinge verhouding met andere grondwetsbepalingen valt tot slot op dat het brief- en telecommunicatiegeheim een uitwerking is van één van de bijzondere aspecten binnen het recht op bescherming van de persoonlijke levenssfeer, te weten de

---

[34] Eindrapport 'Gegevensvergaring in strafvordering' van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, mei 2001.
[35] Zie naast het rapport van de commissie-Mevis ook het oorspronkelijke regeringsvoorstel tot wijziging van artikel 13 uit 1997 (Kamerstukken II 1996/97, 25 443, nr. 2), op welk standpunt het kabinet echter is teruggekomen bij nota van wijziging (Kamerstukken II 1997/98, 25 5443, nr. 6).
[36] *Klass t. Duitsland*, EHRM 6 september 1978, series A 28, par. 55-56.
[37] Kamerstukken II 1997/98, 25 443, nr. 5, blz. 12-16 (nota naar aanleiding van verslag) en Kamerstukken II 1997/98, 25 443, nr. 6 (nota van wijziging).

privé-communicatie (artikel 10). Artikel 13 kent ook in zijn huidige vorm extra waarborgen in de vorm van strengere grondwettelijke competentievoorschriften in vergelijking met artikel 10. De reden voor de ruim geformuleerde beperkingsclausule van artikel 10 is er, zoals blijkt uit de memorie van toelichting bij de grondwetsherziening van 1983, in gelegen dat de persoonlijke levenssfeer een algemeen en ruim begrip was, dat bovendien nog volop in ontwikkeling was. De regering stelde dat het recht op eerbiediging van de persoonlijke levenssfeer op zo uiteenlopende gebieden aan de orde kan komen, dat dit tot gevolg heeft dat de grondwettelijke beperkingsbevoegdheid zodanig geformuleerd moet zijn dat op het zoveel gevarieerder terrein van privacybescherming adequate bewerkingsmogelijkheden beschikbaar dienen te zijn.[38] Het brief- en telecommunicatiegeheim is, anders dan de persoonlijke levenssfeer, wel nader af te bakenen. Deze observatie geldt thans nog steeds, met de toevoeging dat met de diverse telecommunicatietechnologieën de mogelijkheden tot heimelijke inzage niet zijn afgenomen, maar eerder zijn toegenomen.

3.2 Rechterlijke machtiging

Conform het advies van de Staatscommissie Grondwet stellen wij voor de beperkingen op het brief- en telecommunicatiegeheim als hoofdregel alleen toe te staan in gevallen bij de wet bepaald met machtiging van de rechter, met uitzondering van die gevallen waarin de nationale veiligheid in het geding is. Dat betekent een versterking van de waarborgfunctie van de Grondwet.[39] Een toets door de rechter voorafgaand aan de interceptie van communicatie van burgers, denk aan het openen van (elektronische) post, en het tappen van telefoongesprekken of communicatie die verloopt via internet (bijvoorbeeld het natrekken van ingetypte zoekvragen in een internetzoekmachine), heeft een zelfregulerend effect op de uitvoeringspraktijk. Het werpt een natuurlijke drempel op, die naar het oordeel van de regering nodig is om willekeurig gebruik van deze zwaar op de persoonlijke levenssfeer ingrijpende bevoegdheden te voorkomen. Deze toets kan vanuit een oogpunt van *checks and balances* naar het oordeel van de regering het best worden uitgevoerd door een rechter, die vanuit een ander perspectief naar grondrechtelijke beperkingen kijkt dan de uitvoerende macht. Het is immers de uitvoerende macht zelf die wenst over te gaan tot inzage of aftappen van communicatie in het belang van de opsporing van strafbare feiten.

Deze wijziging heeft gevolgen voor de huidige grondwettelijke competentieregeling met betrekking tot het telefoon- en telegraafverkeer. De Grondwet eist op dit moment voor het beperken van het telefoon- en telegraafgeheim immers geen machtiging van de rechter. Voor het op strafvorderlijke titel beperken van het recht op bescherming van dat geheim door het opnemen van telecommunicatie vereist het Wetboek van Strafvordering op dit moment al een voorafgaande schriftelijke machtiging van een rechter (art. 126m, 126t en 126zg Sv). Het voorstel sluit daarmee aan bij de huidige wetgeving en kan aldus worden gezien als een codificatie op grondwetniveau van hetgeen op het niveau van de gewone wet reeds is geregeld.

3.3 Beperkingen in het belang van de nationale veiligheid

[38] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 41
[39] Zo ook het toenmalige kabinet in de nota naar aanleiding van het verslag bij het destijds aanhangige wetsvoorstel, Kamerstukken II 1997/98, 24 553, nr. 5, blz. 13.

Uitzondering op de hoofdregel dat voor beperkingen van het brief- en telecommunicatiegeheim een rechterlijke machtiging nodig is, is dat in het belang van de nationale veiligheid beperkingen zijn toegestaan met machtiging van een of meer ministers die daartoe bij de wet zijn aangewezen. Hiermee wordt aangesloten bij de huidige systematiek van de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002, zie paragraaf 6.3 hierna) voor andere communicatiemiddelen dan de brief, waarvoor nu nog een last van de rechter nodig is. In het verleden heeft het toenmalige kabinet aangevoerd dat de keuze om in deze gevallen een machtiging van de minister in plaats van de rechter te eisen samenhangt met de verantwoordelijkheid van de minister, omdat het gaat om belangrijke beleidsbeslissingen die verband houden met de nationale veiligheid.[40] Deze argumentatie is nog steeds onverkort valide. Bij de uitvoering van de taken die in het kader van de nationale veiligheid aan de inlichtingen- en veiligheidsdiensten zijn opgedragen spelen politiek-bestuurlijke afwegingen een belangrijke rol, waarbij het geheel aan middelen die een inlichtingen- en veiligheidsdienst ter beschikking staan om onderzoek te doen – maar ook de vraag: waarnaar onderzoek te doen – een voortdurende afweging vergt. De minister is in dezen beter geïnformeerd dan de rechter en kan tot een integrale afweging komen. Hieromtrent legt de voor de desbetreffende dienst verantwoordelijke minister uiteindelijk verantwoording af aan het parlement. Het introduceren van een rechterlijke machtiging voor andere communicatiemiddelen dan de brief, zou voorts de (thans beperkte) afwijking van het huidige systeem van de Wiv 2002 verder doen vergroten. Tot slot zou het eisen van een rechterlijke machtiging voor alle intercepties van de inlichtingen- en veiligheidsdiensten noodzaken tot het stellen van specifieke eisen aan de met het verlenen van de desbetreffende rechterlijke machtiging belaste rechtbank; eisen die – enerzijds gelet op het beperkt aantal gevallen per jaar en anderzijds anticiperend op deze grondwetswijziging die daaraan een eind zou maken wat betreft de beperking van het briefgeheim, thans nog niet zijn gesteld. Te denken valt dan bijvoorbeeld aan de concentratie van alle zaken bij een gespecialiseerde rechtbank en eisen in verband met bereikbaarheid en beveiliging.

Delegatie van de machtigingsbevoegdheid is in het voorgestelde artikel 13, tweede lid, evenals in de huidige (oude) bepaling, uitgesloten. De aard van de bevoegdheid, het beperken van het grondwettelijke brief- en telecommunicatiegeheim, is zodanig dat de aangewezen minister te allen tijde degene moet zijn die kan bepalen of een beperking van dat grondrecht noodzakelijk is met een beroep op de nationale veiligheid. Het in delegatie uitoefenen van die bevoegdheid verhoudt zich daar niet mee. Binnen deze systematiek is wel ruimte voor het geven van een machtiging namens de betreffende minister, door middel van mandaat. Dit mandaat wordt uitgeoefend namens, onder verantwoordelijkheid en onder aansturing van de betrokken minister. Het kan te allen tijde ingetrokken worden, en de minister behoudt zelf de bevoegdheid om te besluiten. Als zodanig behoudt de betrokken minister volledige zeggenschap over de wijze waarop deze bevoegdheid wordt uitgeoefend.

De gemaakte uitzondering op de hoofdregel is conform de jurisprudentie van het EHRM. Het EHRM acht – zoals ook de commissie-Franken aangaf – onvermijdelijke inbreuken van inlichtingen- en veiligheidsdiensten op artikel 8 EVRM bij het ontbreken van een rechterlijke machtiging, evenwel slechts gerechtvaardigd wanneer anderszins voldoende voorzien is in 'adequate and effective guarantees against abuse'.[41] Artikel 13 EVRM, dat

[40] Kamerstukken II 1997/98, 25 443 nr. 5, blz. 12-13.
[41] Rapport commissie-Franken, p. 164.

recht geeft op een effectief rechtsmiddel en hier in samenhang met artikel 8 EVRM moet worden bezien, stelt als essentieel vereiste met betrekking tot de inzet van bevoegdheden door inlichtingen- en veiligheidsdiensten die de grondrechten beperken, dat voldoende onafhankelijk toezicht op de diensten noodzakelijk is. Dit toezicht is in het bijzonder belegd bij de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD). Voorts is sprake van parlementaire controle. Eerder zagen ook de commissie-Franken, de Raad van State en de Kamer redenen om voor intercepties in het belang van de nationale veiligheid voor een ander beperkingssysteem te kiezen, gelet op het specifieke karakter van de werkzaamheden van de inlichtingen- en veiligheidsdiensten.

Eén en ander betekent dat het briefgeheim in het belang van de nationale veiligheid voortaan zonder rechterlijke machtiging kan worden beperkt, omdat ook voor het openen van brieven een machtiging van een of meer bij de wet aangewezen ministers volstaat. Dat is een wijziging ten opzichte van het huidige artikel 13, eerste lid, Grondwet, welke eis is uitgewerkt in artikel 23 Wiv 2002, die de rechtbank Den Haag exclusief aanwijst als bevoegd tot het afgeven van een last. Dit kan worden opgevat als een vermindering van de bescherming die het huidige artikel 13 biedt. Wij achten deze wijziging evenwel gerechtvaardigd gelet op de argumenten die hiervoor zijn genoemd. Zoals is opgemerkt in paragraaf 3.1 wil de regering het toestaan van beperkingen bovendien niet langer afhankelijk laten zijn van de gebruikte middelen of technieken. Dat geldt ook voor beperkingen in het belang van de nationale veiligheid.

Waar inbreuken op het brief- en telecommunicatiegeheim in het belang van de nationale veiligheid kunnen plaatsvinden zonder voorafgaande rechterlijke controle is zoals gezegd een adequate alternatieve vorm van toezicht nodig op de toepassing van deze bevoegdheid door de inlichtingen- en veiligheidsdiensten met machtiging van de minister (zie ook paragraaf 6.3 hierna). De Raad van State wijst in zijn advies over het wetsvoorstel uit 2000 op de noodzaak van toezicht op de uitoefening van deze bevoegdheid van de minister, die mede voortvloeit uit de rechtspraak van het EHRM in het licht van artikel 13 EVRM.[42] In dat verband stelde de Raad dat overwogen zal moeten worden dat toezicht grondwettelijk te verankeren (p. 9). Daartoe zien wij geen noodzaak. Wij zijn van mening dat de noodzaak in toezicht te voorzien al in afdoende mate besloten ligt in de clausule dat slechts bij formele wet kan worden bepaald door wie en in welke gevallen de inbreuk mag plaatsvinden. De huidige Wiv 2002 bevat voorts de regeling van (onafhankelijk) toezicht (zie de artikelen 64 en volgende van de wet).[43] Het gaat het sobere karakter van de Grondwet te buiten om aan artikel 13 in dit verband een expliciete opdracht aan de gewone wetgever toe te voegen, luidende dat, voor zover de beperkingen niet aan rechterlijk toezicht kunnen worden onderworpen, bij wet wordt voorzien in een andere vorm van onafhankelijk toezicht. Het EHRM laat zich bovendien niet uit over het niveau – Grondwet of wet - waarop het vereiste toezicht nationaal zou moeten worden geregeld, maar toetst slechts of dergelijk onafhankelijk toezicht in de praktijk bestaat. Internationaal recht vereist aldus niet dat grondwettelijk wordt voorgeschreven dat bij het ontbreken van rechterlijk toezicht wordt voorzien in een andere vorm van onafhankelijk toezicht.

Nationale veiligheid

[42] *Klass t. Duitsland*, EHRM 6 september 1978, series A 28, par. 55-56.
[43] Kamerstukken II 1997/98, 25 877, nr. 3, blz. 77.

In zijn advies van 2002 op het eerdere wetsvoorstel uitte de Raad van State kritiek op het begrip "nationale veiligheid" als doelcriterium voor een ruimere beperkingsmogelijkheid. Volgens de Raad van State zou dit begrip in onvoldoende mate een normatief kader bieden voor beperkingen op het grondrecht. Wij zien dat anders. Zoals reeds door het toenmalige kabinet aangegeven, heeft het begrip "nationale veiligheid" uitwerking gekregen in rechtspraak van het Europees Hof voor de Rechten van de Mens, hoezeer ook op basis van casuïstiek. Zo kan de nationale veiligheid in het geding zijn in geval van het schenden van staats- en militaire geheimen, het oproepen tot het gebruik van geweld, het verrichten van terroristische activiteiten en de publicatie van geschriften die schade kunnen toebrengen aan het functioneren van de staatsveiligheidsdienst van een land. Die uitwerking in de Europese rechtspraak is richtinggevend bij de uitleg van het begrip "nationale veiligheid" in het door ons voorgestane artikel 13. Anders dan de Raad van State zien wij evenmin een probleem in het feit dat het doelcriterium "nationale veiligheid" *de facto* alle werkzaamheden van de veiligheidsdiensten omvat. Op grond van de Wiv 2002 opereren de diensten immers per definitie in het belang van de nationale veiligheid (artikelen 6 en 7). Het begrip "nationale veiligheid" heeft in dit verband dezelfde betekenis als het gelijkluidende begrip in artikel 12 Grondwet en in de wettelijke taakomschrijvingen van de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst op grond van de Wiv 2002. Bij de totstandkoming van die bepalingen is reeds uitvoerig op de betekenis van het begrip ingegaan.[44]

De Raad van State plaatste zijn kritiek op het criterium "nationale veiligheid" ook in het kader van het feit dat dit criterium in het EVRM deel uitmaakt van een breder palet aan beperkingscriteria: naast het doelcriterium van de nationale veiligheid gelden nog andere doelcriteria en bovendien geldt voor al die doelcriteria het vereiste dat de beperking noodzakelijk moet zijn in een democratische samenleving. Een noodzakelijkheidstoets stellen wij in het onderhavige voorstel echter niet voor. Wij kiezen met dit voorstel bewust voor een beperkte modernisering van artikel 13. Dat betekent dat wij de bestaande beperkingssystematiek van de Grondwet ongemoeid laten. In zoverre biedt dit voorstel geen ruimte voor de introductie van een noodzakelijkheidscriterium in artikel 13, zoals de staatscommissie wel voor ogen had door de combinatie met de door haar voorgestelde algemene aanvullende beperkingsclausule.[45] Aan de rechtsbescherming van de burger doet dat intussen niet af: indien de wetgever op het brief- en telecommunicatiegeheim een beperking wenst aan te brengen, dient deze onverkort te worden getoetst aan art. 8 EVRM. In die zin vullen artikel 8 EVRM, dat direct doorwerkt in de nationale rechtsorde, en artikel 13 elkaar aan. Artikel 13 stelt strikte competentievoorschriften – de formele wetgever bepaalt in welke gevallen beperkingen zijn toegestaan met machtiging van respectievelijk de rechter of de minister – en artikel 8 EVRM stelt de materiële beperkingsvereisten van noodzakelijkheid en proportionaliteit met het oog op specifiek omschreven doelcriteria.

4. Regelingsopdracht aan de wetgever

4.1 Horizontale werking

[44] Kamerstukken II 1999/00, 25 877, nr. 8, blz. 18-21 (nota naar aanleiding van verslag) en nr. 9, blz. 13-16 (nota van wijziging), nr. 14 (nota naar aanleiding van het nader verslag), blz. 6-8 en 14-24, nr. 15 (tweede nota van wijziging), blz. 4-5 en nr. 58 (verslag van een wetgevingsoverleg), blz. 31-33.
[45] Zie paragraaf 6.5 en p. 88 van het rapport van de Staatscommissie Grondwet.

Artikel 13 leent zich niet voor directe toepassing in horizontale verhoudingen. De bepaling kent nu, noch in het nieuwe voorstel een direct afdwingbaar recht op bescherming van het brief- en telecommunicatiegeheim van de burger in relatie tot private partijen (bijvoorbeeld de postvervoerder, de werkgever die een intranet beheert of de *Internet Service Provider*). Directe toepassing in de horizontale relatie past niet in het systeem van de Grondwet. Wel leent het grondrechtelijke *belang* – het privé kunnen communiceren zonder dat derden kennis mogen nemen van de inhoud - zich voor horizontale werking in de vorm van een belangenafweging. Een rechter kan diverse grondrechtelijke belangen, waaronder het recht op bescherming van de persoonlijke levenssfeer, ook nu reeds afwegen tegen de rechten en plichten van anderen.[46]

De wetgever verplicht postvervoerbedrijven in artikel 4 van de Postwet om het grondwettelijke briefgeheim niet te schenden. Bovendien kent de Telecommunicatiewet een uitgewerkte borging van het telecommunicatiegeheim in het kader van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten. De Telecommunicatiewet richt zich exclusief op normadressaten die een openbaar karakter hebben. Elektronische netwerken en elektronische diensten met een besloten karakter vallen buiten het bereik van de Telecommunicatiewet. Elektronische communicatienetwerken zoals interne e-maildiensten en toegang tot het intranet van een werkgever zijn voorbeelden van besloten netwerken. Met de constatering dat de Telecommunicatiewet enkel geldt voor openbare netwerken en diensten is het communicatieverkeer dat plaatsvindt in netwerken en diensten met een besloten karakter evenwel niet vogelvrij voor wat betreft hun brief- en telecommunicatiegeheim. In besloten netwerken bieden de beginselbepalingen in het BW (het 'goed werkgeverschap' ex art. 7:611 BW kan indien nodig door de rechter met het belang bij het brief- en telecommunicatiegeheim nader worden ingevuld) en de Wet bescherming persoonsgegevens (Wbp) bescherming. De werksfeer is bijvoorbeeld geen privésfeer, al mogen werknemers binnen grenzen wel een redelijke verwachting van privacy koesteren in hun werkomgeving. Het uitgangspunt van *informed consent* vervult in dat kader een belangrijke rol bij de beoordeling van de beperking van het brief- en telecommunicatiegeheim van de werknemer. Onder deze omstandigheden past in voorkomende gevallen een belangenafweging door de rechter. De Wbp en andere wettelijke bepalingen bieden hiervoor voldoende houvast.

De vraag is, gezien het toenemende en in een groot aantal sectoren exclusieve aandeel van private partijen in de overdracht en eventuele bewaring van berichten, gerechtvaardigd of in de Grondwet een opdracht aan de wetgever moet worden opgenomen met het oog op het waarborgen van het brief- en telecommunicatiegeheim in horizontale verhoudingen. Hoewel een dergelijke grondwettelijke opdracht niet noodzakelijk is voor de wetgever om nadere regels te treffen, pleiten verschillende argumenten voor het opnemen van een regelingsopdracht in de Grondwet. Zoals ook in paragraaf 2.4 is opgemerkt delen wij de visie van de toenmalige regering dat de toegevoegde waarde van een regelingsopdracht vooral is gelegen in het feit dat hiermee de bescherming van het brief- en telecommunicatiegeheim in private verhoudingen tot de aanhoudende zorg van de overheid wordt verklaard, ook met het oog op de mogelijke ontwikkeling van nu nog onbekende communicatiemiddelen- en technieken. Het niet adequaat beschermen van het belang zal mogelijk een ontmoedigend en temperend effect

[46] Zie *Agfa t. Schoolderman*, HR 8 april 1994, NJ 1994, 704 (met betrekking tot de doorwerking van het grondwettelijk discriminatieverbod). Zie ook Pres. Rb. Roermond, 12 september 1985, KG 1985, 299 en Hof Den Bosch, 2 juli 1986, NJ 1987, 451 (met betrekking tot de doorwerking van privacy). Zie verder *KLM t. Reinders*, Ktg. Haarlem 16 juni 2000, JAR 2000-170 (privacy)

hebben op het ongehinderd en privé communiceren, maar ook op het genot van andere grondrechten, zoals de persoonlijke levenssfeer en vrije informatiegaring zijn uitwerking doen gevoelen omdat burgers zich niet meer vrij voelen om zonder een meekijkende derde te communiceren en informatie te vergaren. Het kan nodig zijn ter bescherming van het brief- en telecommunicatiegeheim regels te stellen aan degenen die de communicatiemiddelen beheren om dat geheim ook daadwerkelijk en effectief te borgen.

Ook kan over de contractuele relatie tussen gebruiker en de derde die het beheer heeft over de communicatie nadere bezinning aangewezen zijn. Vaak zal instemming van de gebruiker over het inzien van de communicatie geschieden door aanvaarding van de algemene voorwaarden van een bedrijf (*informed consent*). Daarbij kan het in de toekomst nodig zijn dat de wetgever de burger ondersteunt met bepaalde effectieve rechten van de burger en plichten van bedrijven, gelet op de machtige positie van bijvoorbeeld internetbedrijven.[47] Contractuele afspraken waarborgen immers niet altijd een goed geïnformeerde beslissing van de gebruiker. Een informatieachterstand bij de gebruiker, de complexiteit van de door de aanbieder gebruikte techniek en het bestaan van keuzedwang – zonder instemming immers geen toegang tot de gewenste informatie – kunnen de beslissing van de gebruiker beïnvloeden. Vanwege de zich steeds voordoende grootschalige wijzigingen op het terrein van communicatietechnologie dient de wetgever voortdurend alert te zijn op nieuwe technologieën en nieuwe toepassingen in het elektronische communicatieverkeer, opdat burgers adequaat worden beschermd tegen ongebreidelde inzage door private partijen. Het voorgestelde derde lid geeft een algemene regelingsopdracht aan de wetgever, welke onder meer gericht is op het regelen van de bescherming van het brief- en telecommunicatiegeheim in horizontale verhoudingen.

4.2 Notificatie

Degene op wiens brief- of telecommunicatiegeheim inbreuk wordt gemaakt, heeft er in beginsel aanspraak op daaromtrent te worden geïnformeerd. De Staatscommissie Grondwet heeft in 2010 echter zonder nadere toelichting afgezien van een notificatieplicht. Thans kiest de regering voor een algemene regelingsopdracht aan de wetgever in het derde lid van het onderhavige voorstel. Deze regelingsopdracht laat ruimte aan de formele wetgever om een notificatieplicht te regelen. Het kan in voorkomende gevallen noodzakelijk zijn, de balans tussen enerzijds de mate van noodzakelijke heimelijkheid voorafgaand aan observatie of inzage en een effectieve bescherming van het recht op het brief- en communicatiegeheim, achteraf te herstellen met een notificatieplicht. De regelingsopdracht laat ook ruimte om in geval van de opsporing van strafbare feiten of onderzoeken in het belang van de nationale veiligheid te regelen dat de notificatie indien nodig kan worden uitgesteld of – in laatstgenoemd geval – zelfs af te stellen. In dit verband heeft de CTIVD ook de vraag gesteld of de kosten van de tenuitvoerlegging van de notificatieplicht opwegen tegen de baten. Het gaat hierbij – ook volgens de CTIVD – om het maken van afwegingen waartoe de wetgever geroepen is. Deze kan naar onze mening het beste bepalen in welke gevallen de notificatieplicht een meerwaarde heeft voor het Nederlandse systeem van rechtsbescherming.[48]

---

[47] Zie bijvoorbeeld art. 11.7a Tw (het cookieverbod).

[48] Zie toezichtsrapport van de commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD) inzake de rechtmatigheid van de uitvoering van de notificatieplicht door de AIVD, rapport nr. 24 2009, p. 31.

5. Verhouding tot internationale regelgeving

5.1 EU

Handvest van de grondrechten van de Europese Unie

Het brief- en telecommunicatiegeheim is beschermd in artikel 7 van het Handvest van de Grondrechten van de Europese Unie (hierna: EU-Handvest). Het luidt: 'Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie'. In de toelichting bij het EU-Handvest staat dat de in artikel 7 gewaarborgde rechten corresponderen met de rechten die in artikel 8 van het EVRM zijn gewaarborgd. Om rekening te houden met de technische ontwikkelingen is het woord 'correspondentie' in het EU-Handvest vervangen door 'communicatie'.[49] Naar verwachting zal het Hof van Justitie van de EU het begrip 'communicatie' invulling geven langs de lijnen van het Europese Hof voor de Rechten van de Mens (EHRM).[50] Een toegevoegde waarde van deze bepaling in het Handvest is gelegen in het feit dat de EU op grond van haar supranationaliteit kan afdwingen dat maatregelen ook worden toegepast in grensoverschrijdende situaties. Tegelijkertijd moet het, wil een beroep op artikel 7 EU-Handvest slagen, altijd om een situatie gaan die wordt bestreken door Europese wetgeving. Artikel 8 EU-Handvest is een lex specialis van artikel 7 EU-Handvest, en ziet op het recht op bescherming van persoonsgegevens.

Secundair EU-recht

In het secundaire EU-recht zijn in verband met het brief- en telecommunicatiegeheim vooral de algemene privacy-Richtlijn 95/46/EG (hierna: Privacyrichtlijn)[51] en de meer specifieke Richtlijn 2002/58/EG die ziet op de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (hierna: ePrivacyrichtlijn) van belang. De beide Richtlijnen zijn ieder op hun eigen wijze van belang voor de inhoud van het brief- en telecommunicatiegeheim.

De Privacyrichtlijn ziet allereerst op de wijze waarop persoonsgegevens moeten worden beschermd en is ten aanzien van twee aspecten relevant. Allereerst ziet het op de wijze waarop persoonsgegevens, dus tot personen herleidbare gegevens, dienen te worden beschermd. Hoewel de Privacyrichtlijn wel naar communicatienetwerken verwijst[52], bevat de Privacyrichtlijn als zodanig geen specifieke regels voor telecommunicatie.[53] Daarnaast is de Privacyrichtlijn van betekenis voor de bescherming van verkeersgegevens. Verkeersgegevens zijn, voor zover ze tot een persoon herleidbaar zijn, immers persoonsgegevens.

---

[49] 2007/C303/02.
[50] Zie voor de interpretatie van het EU-Handvest in het licht van het EVRM art. 51-54 van het EU-Handvest, en specifiek art. 52 lid 3..
[51] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. De Privacyrichtlijn zal in 2013 naar alle waarschijnlijkheid worden omgezet in een Verordening.
[52] Zie overwegingen 6 en 47 bij de Privacyrichtlijn.
[53] De richtlijn kent enkel de voorwaarde dat indien een boodschap met persoonsgegevens via een telecommunicatienetwerk of via een telecommunicatiedienst wordt verzonden en de functie van de telecommunicatiedienst enkel bestaat uit de overdracht van berichten, ervan wordt uitgegaan dat degene die het bericht verzendt, de 'verantwoordelijke' is in de zin van de Privacyrichtlijn

Voor verkeersgegevens die worden gegenereerd bij de overdracht van berichten is verder ook de Richtlijn betreffende bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten (hierna: Dataretentierichtlijn).[54] Deze richtlijn harmoniseert nationale bepalingen van de lidstaten waarbij aan aanbieders van elektronische communicatiediensten of –netwerken bewaarverplichtingen worden opgelegd. Deze verplichting tot bewaring van verkeersgegevens kunnen alleen worden gevorderd in het kader van het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgeving. Verwerking van verkeersgegevens door telecomaanbieders ten behoeve van de overheid is dus onder strikte condities in de Dataretentierichtlijn toegestaan.

Naast het algemene kader van de Privacyrichtlijn werd een specifiek op de telecommunicatiesector toegesneden regeling noodzakelijk geacht. De ePrivacyrichtlijn, een lex specialis van de Privacyrichtlijn, beschermt de persoonlijke levenssfeer van gebruikers van openbare elektronische communicatienetwerken en -diensten.[55] Hoewel de ePrivacyrichtlijn werking in verticale verhoudingen niet uitsluit, beheerst deze vooral horizontale rechtsrelaties. De aanbieders van openbare elektronische communicatienetwerken en -diensten zijn voor het overgrote deel (en in Nederland exclusief) immers private ondernemingen. Het doel van de ePrivacyrichtlijn is tweeledig: bescherming van de fundamentele rechten en vrijheden van natuurlijke personen en rechtmatige belangen van rechtspersonen in verband met de steeds grotere mogelijkheid tot geautomatiseerde verwerking van gegevens buiten het zicht van de gebruiker, en het borgen van het vertrouwen van de gebruikers, dat hun persoonlijke levenssfeer ook bij verdergaande grensoverschrijdende ontwikkelingen worden beschermd. Activiteiten die verband houden met de openbare veiligheid, defensie, staatsveiligheid en strafrechtelijke opsporing en vervolging vallen buiten het bereik van de e-Privacyrichtlijn. De reikwijdte van de ePrivacyrichtlijn strekt zich uit over openbare elektronische netwerken en diensten. De zogenoemde besloten elektronische netwerken vallen er niet onder; deze worden wel beschermd door de algemene Privacyrichlijn. De algemene Privacyrichtlijn is geïmplementeerd in de Wet bescherming persoonsgegevens, de ePrivacyrichtlijn is omgezet in de Telecomunicatiewet (Tw) en de Dataretentierichtlijn is tot slot opgenomen in de Tw en de Wet op de economische delicten.[56] Het voorgestelde artikel 13 staat niet op gespannen voet met de vigerende EU-bepalingen. De in de Wbp en Tw opgenomen EU-uitgangspunten zijn veeleer een nadere uitwerking van de te beschermen belangen waarop het grondwettelijke brief- en telecommunicatiegeheim ziet. In die zin vormen ze een waardevolle uitwerking die het rechtens te beschermen belang – het privé kunnen communiceren – daadwerkelijk en effectief in horizontale relaties te beschermen.

5.2 Internationale verdragen

In de Nederlandse rechtsorde zijn verschillende internationale verdragen van toepassing

[54] Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG.
[55] Zie Richtlijn 2002/58/EG van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie. Deze Richtlijn is naderhand gewijzigd door Richtlijn 2009/136/EG van 25 november 2009 tot wijziging van […] Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie […].
[56] Wet bewaarplicht telecommunicatiegegevens, Kamerstukken I 2007/08, 31 145, nr. A.

die het equivalent van het grondwettelijke brief- en telecommunicatiegeheim beschermen. De internationale verdragen spelen in de Nederlandse rechtspraktijk een belangrijke rol, onder meer vanwege de directe doorwerking van het EU-recht in de Nederlandse rechtsorde, en het feit dat de Nederlandse rechter formele wetten niet aan de Grondwet, maar wel aan een ieder verbindende bepalingen van verdragen kan toetsen op grond van de artikelen 93 en 94 Grondwet. Waar op één en hetzelfde vraagstuk verschillende normenstelsels van toepassing zijn, doet zich het risico voor van onzekerheid en onduidelijkheid ten aanzien van de onderlinge verhouding van die stelsels. In deze paragraaf gaan wij daarom nader in op het brief- en telecommunicatiegeheim in internationale context. In internationale verdragen kent het brief- en telecommunicatiegeheim geen afzonderlijke regeling. De internationale dimensie van het recht op respect voor het brief- en telecommunicatiegeheim is belichaamd in art. 8 EVRM en art. 17 IVBPR. Art. 17 IVBPR kent geen beperkingsgronden of –criteria. Van deze beide artikelen heeft art. 8 EVRM de meest vergaande invloed op de bescherming van het recht op het huidige brief- telefoon- en telegraafgeheim.

De jurisprudentie van het EHRM heeft aan de betekenis van art. 8 EVRM een belangwekkende bijdrage geleverd. Het brief- en telecommunicatiegeheim wordt beschermd door art. 8 EVRM, dat 'privacy' en 'correspondence' noemt. 'Correspondence' kent hetzelfde beschermingsregime als de persoonlijke levenssfeer die als eerste wordt genoemd in art. 8. De verdragsstaten bij de Raad van Europa zijn in beginsel vrij in de wijze waarop zij de rechten en vrijheden uit de verdragen implementeren zolang de materiële betekenis ervan wordt geborgd.

Uit het verdrag zelf kan niet worden afgeleid welke vormen communicatie worden beschermd. Het recht op respect voor 'correspondence' kwam in eerste instantie tot ontwikkeling in de jurisprudentie in een aantal zaken waarin het recht op privé-communicatie van gedetineerden afgebakend diende te worden. Later heeft het EHRM steeds op basis van casuïstiek geoordeeld of aanspraken op het recht op respect voor correspondentie onder andere omstandigheden onder de reikwijdte van artikel 8 EVRM vielen.[57] Het Hof heeft het recht op respect voor 'correspondence' steeds uitgelegd tegen de achtergrond van de andere rechten in het spectrum van artikel 8 (respect voor het privé-leven en voor de woning).

De bescherming van artikel 8 en in het bijzonder van het recht op respect op correspondentie ziet volgens de jurisprudentie in ieder geval ook op inhoud van berichten die via communicatiemiddelen worden overgebracht. Het Hof verwierp in *A. t. Frankrijk* het verweer van de staat dat geen inbreuk gemaakt zou op artikel 8 EVRM, omdat volgens de staat een telefoonconversatie over criminele activiteiten buiten het bereik van artikel 8 zou vallen. Met deze benadering stemde het Hof niet in. De specifiek geuite inhoud van het telefoongesprek, in casu het voornemen van criminele activiteiten, doet voor de gelding van artikel 8 EVRM aldus niet ter zake, wel het feit dat de communicatie via een communicatiemiddel, in dit geval de telefoon, verliep.[58] De specifieke inhoud van communicatie, in dit geval de conversatie over de criminele activiteiten, kan geen aanleiding zijn om het brief- en telecommunicatiegeheim in dit geval op te heffen. Deze benadering sluit aan bij het voorgestelde brief- en telecommunicatiegeheim dat ziet op het beschermen van het middel waarmee de communicatie tot stand wordt gebracht.

Uit de jurisprudentie blijkt dat het Hof voor een benadering kiest waarin ruimte is voor

---

[57] Zie onder meer *Golder t. Verenigd Koninkrijk*, EHRM 21 februari 1975, series A 18, *Klass t. Duitsland*, EHRM 6 september 1978, series A 28 en *Silver t. Verenigd Koninkrijk*, 25 maart 1983 series A 61.
[58] *A. t Frankrijk*, EHRM 23 november 1993, series A vol 277-B, par. 34 e.v..

telecommunicatie als onderdeel van 'privé-leven' alsook als onderdeel van 'correspondentie'.[59] Het gaat daarbij om communicatie die naar zijn aard in ieder geval geadresseerd, ofwel gericht is. Communicatie die plaatsvindt in een besloten netwerk, zoals bijvoorbeeld binnen het netwerk van een werkgever, valt eveneens onder de reikwijdte van artikel 8 EVRM.[60] Een werknemer komt blijkens de EHRM-jurisprudentie een redelijke privacyverwachting toe, tenzij deze er uitdrukkelijk op is gewezen dat en onder welke voorwaarden controle van bijvoorbeeld internetgebruik, e-mail en telefoonverkeer plaatsvindt.[61]

Artikel 8 EVRM verlangt in het geval van een beperking een voor eenieder toegankelijke en voorzienbare regeling die het recht op privacy beperkt in het belang van de het tweede lid van artikel 8 EVRM genoemde doeleinden en die noodzakelijk is in een democratische samenleving, hetgeen inhoudt dat de beperking proportioneel moet zijn in verhouding tot het doel dat ermee wordt gediend. Nationale veiligheid, openbare orde of het economisch welzijn van het land, voorkoming van wanorde of strafrechtelijke gedragingen, bescherming van de gezondheid of van de moraal, of bescherming van de rechten en vrijheden van anderen vormen een legitieme grondslag voor beperkingen. Artikel 8 EVRM is techniekonafhankelijk geredigeerd en gaat uit van algemene, materiële beperkingseisen. Artikel 13 Grondwet laat beperkingen toe op grond van competentiecriteria, door een formeelwettelijke grondslag en een machtiging van de rechter, respectievelijk een of meer ministers, te eisen.

Wij zien het verschil in de aard van de door het EVRM en de Grondwet gestelde beperkingseisen niet als een probleem. De internationale verdragen leggen minimumnormen vast waaraan lidstaten moeten voldoen. Op nationaal niveau kan gekozen worden voor een meer uitgebreide bescherming van in dit geval het brief- en telecommunicatiegeheim. Bepalend is immers het beginsel dat de verschillende stelsels cumulatief werken: datgene waaraan de burger de meeste bescherming kan ontlenen bepaalt zijn rechtspositie. De internationale verdragen zijn complementair aan het huidige en het onderhavige voorstel voor de wijziging van artikel 13.

6. Verhouding tot nationale wetgeving

6.1 Grondwetssystematiek en grondrechten

Kenmerkend voor onze Grondwet is dat zij een sober en open karakter heeft. Er is uitdrukkelijk niet voorzien in uitputtende regelingen. Daarnaast kenmerkt de Grondwet zich door een verzwaarde procedure tot wijziging vanwege onder meer de versterkte meerderheidseis. De Grondwet bevat regels ter waarborging en bevordering van de vrijheid en het welzijn van de burgers, en legt de voornaamste elementen en fasen vast van de politieke wils- en besluitvorming.[62] Zij biedt het kader en de grondregels waarbinnen de uitoefening van overheidmacht dient plaats te vinden. Zij ziet aldus primair op verticale rechtsrelaties.

Tegen de achtergrond van de geringe veranderbaarheid, de soberheid en de openheid van de Grondwet dienen wijzigingen voornamelijk tot beslechting van langdurig lopende en politiek omstreden thema's. Aanpassingen moeten door de samenleving breed worden

[59] *Copland t. Verenigd Koninkrijk*, EHRM 3 april 2007. Zowel e-mail als het bezoek van pagina's op het internet werden geacht onder de reikwijdte van artikel 8 te worden beschermd.
[60] *Halford t. Verenigd Koninkrijk*, EHRM 27 mei 1997.
[61] *Copland t. Verenigd Koninkrijk*, EHRM 3 april 2007.
[62] Vgl. *Kamerstukken II* 2010-2011, nr. 20, p. 2 en Commissie Franken (2000), p. 46.

gedragen, hetgeen zich uit in de vereiste meerderheden in de besluitvormingsprocedures. Zij moeten bovendien zijn ingegeven door een maatschappelijke en juridische noodzaak. Bovendien moet het gaan om zaken die voldoende constitutionele rijpheid vertonen.[63] Artikel 13 behoeft vanwege zijn gesloten formulering en de ontwikkelingen in de gedigitaliseerde informatiesamenleving zoals hiervoor geduid, dringend wijziging. De onzekerheid over de reikwijdte kan niet voldoende worden gepareerd met extensieve interpretatie van artikel 13. Bovendien levert het betreffende artikel sinds lange tijd politieke en juridische discussie op.[64]

Artikel 13 is een lex specialis van artikel 10. Artikel 10 beschermt het recht op de persoonlijke levenssfeer en vormt een inleiding niet alleen gericht op de volgende leden van artikel 10, maar ook op het in de artikelen, 11, 12 en 13 bepaalde. Artikel 13 omvat een specifieke regeling voor privé communicatie. De toegevoegde waarde van artikel 13 ten opzichte van artikel 10 Grondwet is gelegen in het feit dat artikel 13 voor dit specifieke aspect van de persoonlijke levenssfeer, te weten de privé-communicatie een eigen beschermingsregime biedt. Op dit moment vergt artikel 13 een rechterlijke last voor de opening en kennisneming van brieven en de machtiging van een bij wet aangewezen personen voor het tappen van telefoon en telegraaf. Artikel 10 kent een vergelijkbare last voor de kennisneming van persoonsgegevens door de overheid thans niet.

Op het niveau van de grondslag bestaat een duidelijk verband tussen artikel 7 Grondwet (vrijheid van meningsuiting) en artikel 13. Beide artikelen zien op het belang van bescherming van communicatie. Artikel 7 beschermt de vrijheid van het uiten van gedachten en gevoelens in het openbaar en vrijwaart de inhoud van de uiting tegen inmenging door de overheid middels het censuurverbod en richt zich daarmee op het belang bij communicatievrijheid. Artikel 13 beschermt uiting van gevoelens en gedachten in privé-communicatie; de inhoud van de communicatie wordt hier beschermd tegen openbaarheid en tegen kennisneming ervan de overheid en richt zich op het communicatiegeheim. Het verschil in gerichtheid van de communicatie tussen de vrijheid van meningsuiting en het brief- en telecommunicatiegeheim is hierin doorslaggevend voor de gelding van het ene of het andere aspect van communicatie.

6.2 Strafrecht

Veel beperkingen op het brief- en telecommunicatiegeheim, alsook de eisen die daaraan worden gesteld, zijn vervat in het wetboek van Strafrecht en het wetboek van Strafvordering. Het strafrecht draagt ook bij aan de bescherming van het brief- en telecommunicatiegeheim in horizontale verhoudingen, door onder meer computervredebreuk (artikel 138ab Sr.), het door middel van apparatuur afluisteren van binnen en buiten gevoerde gesprekken (resp. artikel 139a en artikel 139b Sr.), en het aftappen of opnemen van telefoongesprekken of bestanden (artikel 139c Sr.) strafbaar te stellen. Voorts is het onttrekken van brieven of andere poststukken aan hun bestemming (art. 201 Sr), en schending van het brief- en telecommunicatiegeheim door medewerkers van post- en openbare telecommunicatie bedrijven (art. 273a-273d en 371 Sr) strafbaar gesteld. Deze strafbepalingen illustreren het belang van het brief- en telecommunicatiegeheim, ook in horizontale verhoudingen.

Dit wetsvoorstel houdt in dat het vereiste van een voorafgaande rechterlijke machtiging, dat thans alleen voor beperkingen van het recht op bescherming van het

[63] *Kamerstukken II* 2010-2011, nr. 20, p. 4.
[64] *Kamerstukken II* 2010-2011, nr. 20, p. 10.

briefgeheim geldt, ook gaat gelden voor beperkingen van het recht op bescherming van het telecommunicatiegeheim. Het Wetboek van Strafvordering maakt beperking van het recht op bescherming van het telecommunicatiegeheim voor strafvorderlijke doeleinden mogelijk. Op grond van de artikelen 126m, 126t en 126ng Sv kan telecommunicatie die verloopt via de telefoon of het internet worden getapt. Daarnaast kent dat wetboek de mogelijkheid om onder nadere voorwaarden van de aanbieder van een communicatiedienst te vorderen dat deze andere gegevens dan verkeersgegevens of gebruikergegevens verstrekt. Het gaat daarbij om gegevens waar de aanbieder de toegang toe heeft maar die niet voor hem zelf zijn bestemd of van hem afkomstig zijn. Het betreft gegevens die klaarblijkelijk van de verdachte afkomstig zijn, voor de verdachte bestemd zijn, op de verdachte betrekking hebben of tot het begaan van het strafbare feit hebben gediend, of met betrekking tot welke gegevens het strafbare feit klaarblijkelijk is gepleegd (zie de artikelen 126ng, 126ug en 126zo Sv). Een voorbeeld van een dergelijk gegeven is de inhoud van een van de verdachte afkomstige e-mail die op een webserver staat. Omdat het tappen van telecommunicatie en het vorderen van gegevens waar de aanbieder van een communicatiedienst toegang toe heeft worden gezien als diep in de persoonlijke levenssfeer ingrijpende opsporingsbevoegdheden stelt het wetboek van Strafvordering strikte voorwaarden aan de inzet van deze bevoegdheden. Zij kunnen alleen worden uitgeoefend in geval van verdenking van misdrijven van een zekere ernst. Daarnaast geldt voor al deze bevoegdheden dat deze slechts met een voorafgaande schriftelijke machtiging van de rechter-commissaris, op vordering van de officier van justitie verleend, kunnen worden uitgeoefend.

Ook voor verkeersgegevens die geheel of ten dele mede betrekking hebben op de inhoud van de communicatie, zoals de onderwerpregel van een e-mail en de in een internetzoekmachine ingevoerde zoekterm (zie hierboven in paragraaf 2.3), geldt dat deze slechts met een voorafgaande schriftelijke machtiging van de rechter-commissaris, op vordering van de officier van justitie verleend, kunnen worden gevorderd. De artikelen 126ng, 126ug en 126zo Sv betreffen andere gegevens dan verkeersgegevens en gebruikergegevens. Als verkeersgegevens zijn krachtens de artikelen 126n, 126u en 126zh Sv (in het Besluit vorderen gegevens telecommunicatie) alleen gegevens aangewezen die niet geheel of ten dele mede op de inhoud van de communicatie betrekking hebben. Doordat gegevens zoals de onderwerpregel van een e-mail en de in een internetzoekmachine ingevoerde zoekterm niet als verkeersgegevens zijn aangewezen, geldt voor het vorderen van deze gegevens het zwaardere regime van de artikelen 126ng, 126ug en 126zo Sv waaronder onder meer een voorafgaande schriftelijke machtiging van de rechter-commissaris.

Op grond van het voorgaande heeft het voorgestelde nieuwe artikel 13 geen gevolgen voor de huidige strafrechtelijke wetgeving. Deze wetgeving is reeds in overeenstemming met de eis dat beperkingen op het brief- en telecommunicatiegeheim in beginsel slechts kunnen plaatsvinden met een rechterlijke machtiging.

Opmerking verdient tot slot dat het recht op bescherming van het brief- en telecommunicatiegeheim van personen die rechtmatig van hun vrijheid zijn beroofd verdergaand kan worden beperkt op grond van artikel 15, vierde lid, van de Grondwet, dan op grond van het voorgestelde artikel 13, tweede lid, mogelijk is. Op grond van de Penitentiaire beginselenwet, de Beginselenwet verpleging ter beschikking gestelden en de Beginselenwet justitiële jeugdinrichtingen kan de directeur van de inrichting op in die wetten genoemde gronden en onder de daarin gestelde voorwaarden beperkingen op het bedoelde recht aanbrengen, zonder dat de uitoefening van die bevoegdheden afhankelijk is gesteld van een machtiging van de rechter.

6.3 Wet op de inlichtingen- en veiligheidsdiensten 2002

De bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten (AIVD en MIVD) kunnen inbreuk maken op grond- en mensenrechten, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, en mogen daarom alleen onder strikte voorwaarden worden uitgeoefend. Bevoegdheden uit de Wiv 2002 die specifiek kunnen ingrijpen in het brief- en telecommunicatiegeheim zijn het openen van brieven (art. 23), het binnendringen in een geautomatiseerd werk (art. 24), het gericht aftappen van elke vorm van gesprek, telecommunicatie of gegevensoverdracht (art. 25) en het ongericht ontvangen en opnemen alsmede selecteren van niet-kabelgebonden telecommunicatie (art. 26 en 27). Ook mogen de diensten zich wenden tot aanbieders van openbare telecommunicatienetwerken en telecommunicatiediensten in de zin van de Telecommunicatiewet met het verzoek gegevens te verstrekken over het telecommunicatieverkeer met betrekking tot een gebruiker (art. 28 en 29). De inlichtingen- en veiligheidsdiensten mogen bijzondere bevoegdheden of inlichtingenmiddelen slechts toepassen, indien dat noodzakelijk is voor de goede uitvoering van de aan de diensten opgedragen taken (art. 18 Wiv 2002) en met inachtneming van de eisen van proportionaliteit (art. 31 Wiv 2002) en subsidiariteit (art. 32 Wiv 2002). Dat betekent dat de uitoefening van de bevoegdheden of inlichtingenmiddelen in een goede verhouding moeten staan tot het doel waarvoor ze worden ingezet en alleen mogen worden gebruikt als dat resultaat niet met andere, minder ingrijpende bevoegdheden kan worden bereikt. De Minister van Binnenlandse Zaken en Koninkrijksrelaties onderscheidenlijk de Minister van Defensie, of namens deze het hoofd van de desbetreffende dienst, moet voor zover de wet niet anders bepaalt toestemming geven voor het uitoefenen van een bijzondere bevoegdheid (art. 19 Wiv 2002). De Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt toezicht op de rechtmatige uitoefening van de bevoegdheden die aan de diensten in de Wiv 2002 zijn toegekend. De voorgestelde bepaling in artikel 13, tweede lid, sluit aan bij dit bestaande wettelijke systeem, in het bijzonder voor de beperkingen in het belang van de nationale veiligheid. Enkel de bepaling die nu nog eist dat voor het openen van brieven een last van de rechtbank Den Haag nodig is, zal moeten worden aangepast aan de nieuwe grondwettelijke beperkingsclausule na inwerkingtreding van dit wetsvoorstel. Voor het openen van brieven volstaat immers onder het onderhavige voorstel een machtiging van een bij de wet aangewezen minister.

6.4 Telecommunicatiewet en Postwet 2009

De Telecommunicatiewet (hierna: Tw) stelt in het kader van de dienstverlening in openbare netwerken strikte voorwaarden om het privé-karakter van elektronische communicatie te waarborgen. Het is onvermijdelijk dat aanbieders het beheer verkrijgen zolang de overdracht van de inhoud van de communicatie duurt. De gebruiker wordt door de Tw beschermd tegen ongebreidelde inzage van zijn communicatie. De bescherming van het telecommunicatiegeheim in de Tw is grotendeels op de ePrivacyrichtlijn gestoeld.

Art. 18.13 lid 1 Tw bevat een instructie van de wetgever aan de lagere wetgever en de uitvoerende instanties om bij het nemen van maatregelen en het stellen van regels bij of krachtens de Tw het belang van de bescherming van de persoonsgegevens en de

bescherming van de persoonlijke levenssfeer alsmede de bescherming van het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechieken in acht te nemen. Het tweede lid van art. 18.13 Tw verklaart het eerste lid van overeenkomstige toepassing op de bedrijfsvoering door aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten. Aanbieders mogen aldus op grond van dit tweede lid geen kennis nemen van de inhoud van de communicatie of verkeersgegevens verwerken, tenzij dat uitdrukkelijk bij of krachtens de Tw is toegestaan.

Art. 11.5 Tw geeft regels voor de verwerking van verkeersgegevens door de aanbieders van openbare elektronische communicatiediensten en –netwerken. De Tw volgt daarmee letterlijk de definitie zoals die is neergelegd in de ePrivacyrichtlijn en kent een niet-limitatieve lijst van verkeersgegevens: 'gegevens die worden verwerkt voor het overbrengen van communicatie van communicatie over een elektronisch communicatienetwerk of voor de facturering daarvan'.[65] Het beschermingsregime voor de verwerking van verkeersgegevens dat in de ePrivacyrichtlijn en in de Tw is neergelegd is strikt. Ook aan het benutten van de locatiegegevens van de eindapparatuur van de gebruiker stelt art. 11. 5a van de Tw voorwaarden. Zowel verkeersgegevens als locatiegegevens mogen slechts voor een beperkte termijn worden bewaard. Na gebruik in het kader van de in de Tw genoemde doeleinden dienen deze te worden verwijderd of te worden geanonimiseerd. Toestemming van de gebruiker is noodzakelijk in het kader van verwerking van locatiegegevens door de aanbieder. Bij verkeersgegevens speelt het toestemmingsvereiste wanneer de aanbieder met behulp van de verkeersgegevens wil overgaan tot levering van toegevoegde waardediensten. Bij zowel de verkeersgegevens als bij de locatiegegevens moet de gebruiker te allen tijde zijn toestemming kunnen intrekken.

In het belang van de nationale veiligheid of de voorkoming, opsporing en vervolging van strafbare feiten kan beperking van de rechten van de gebruiker met betrekking tot de verkeersgegevens aangewezen zijn. Gelet op de systematiek van de Tw kunnen aanbieders [de] bescherming die voortvloeit uit art. 11.5a enkel buiten toepassing laten indien zij op grond van Hoofdstuk 13 Tw gehouden zijn tot medewerking. In dergelijke gevallen gaat het aldus om inzage in de verkeers- en locatiegegevens en de daarmee verband houdende gegevens die noodzakelijk zijn om de gebruiker te identificeren. Het kennis nemen van de inhoud van de communicatie in het belang van de nationale veiligheid of de voorkoming, opsporing en vervolging van strafbare feiten bij de aanbieder van de openbare elektronische communicatiedienst of –netwerk is enkel toegestaan binnen het regime van artikel 13 Grondwet.

Tot slot kan niet onvermeld blijven dat een nieuw art. 11.2a zal worden opgenomen in de Tw. Volgens dit artikel dragen aanbieders van een openbare elektronische communicatiedienst en/of –netwerk zorg voor het privé-karakter van de inhoud van de communicatie en de daarmee verband houdende gegevens (verkeers- en locatiegegevens) via hun netwerken onderscheidenlijk hun diensten.[66] Uitzonderingen hierop dienen immer noodzakelijk en proportioneel te zijn. Indien een aanbieder derden inschakelt voor het verrichten van werkzaamheden blijft de aanbieder verantwoordelijk voor een goede dienstverlening aan de gebruikers en voor naleving van wettelijke verplichtingen. In de afspraken met de uitvoerende partij dient de aanbieder te voorzien in het waarborgen van de naleving van de in dit artikel opgenomen verplichtingen. De Opta ziet samen met het College bescherming persoonsgegeven toe op de naleving van de bepalingen in hoofdstuk 11 van de Telecommunicatiewet inzake de bescherming van persoonsgegevens en de

[65] Art. 11.1 sub b Tw.
[66] Art. 11.2a implementeert art. 5, eerste en tweede lid van de ePrivacyrichtlijn.

persoonlijke levenssfeer.

Net als in het Wetboek van Strafrecht zijn aldus ook bepalingen in de Telecommunicatiewet opgenomen die erop zijn gericht te voorkomen dat de aanbieder inbreuk maakt op het telecommunicatiegeheim.[67] De huidige Telecommunicatiewet verhoudt zich goed tot het voorstel voor het nieuwe artikel 13 en geeft reeds uitvoering aan de regelingsopdracht in het derde lid. Voor wat betreft de openbare elektronische netwerken en –diensten vullen deze bepalingen in de Telecommunicatiewet immers een groot deel van de lacunes in de bescherming van het brief- en telecommunicatiegeheim in horizontale verhoudingen. Gesloten elektronische netwerken zoals bijvoorbeeld netwerken van werkgevers vallen evenwel niet onder de reikwijdte van de Telecommunicatiewet; zij worden thans bestreken door de Wbp en de relevante bepalingen in het BW.

In de artikelen 4 tot en met 6 van de Postwet 2009 is geregeld dat postvervoerbedrijven de aan hen toevertrouwde poststukken vertrouwelijk behandelen. Onder poststukken in de zin van de Postwet 2009 vallen brieven en andere – in het Postbesluit 2009 – aangewezen geadresseerde poststukken. Artikel 4 van de Postwet legt de postvervoerbedrijven een zorgplicht op om hun bedrijfsvoering en het postvervoer zo in te richten dat het grondwettelijk briefgeheim niet wordt geschonden. De postvervoerbedrijven hebben daarbij ruimte om die maatregelen te nemen die passen bij hun bedrijfsvoering en producten zolang het grondwettelijk briefgeheim met die maatregelen gewaarborgd is. Dit betekent onder meer dat maatregelen genomen moeten worden om ervoor te zorgen dat sorteercentra niet voor een ieder toegankelijk zijn. Op grond van artikel 5 is het openen van onbestelbare post alleen toegestaan op last van de rechter. De gegevens in het poststuk mogen uitsluitend worden gebruikt om het poststuk alsnog te kunnen afleveren of te retourneren. Beslag op poststukken is op grond van artikel 6 van de Postwet 2009 alleen mogelijk voor zover de wet dat uitdrukkelijk regelt. Deze wettelijke bepalingen verzekeren voor poststukken die worden verstuurd via postvervoerbedrijven – in aanvulling op artikel 13 – dat ook in horizontale verhoudingen het briefgeheim gewaarborgd is. Deze bepalingen in de Postwet geven aldus uitvoering aan de regelingsopdracht in artikel 13, derde lid.

7. Administratieve lasten en uitvoeringskosten

PM

8. Consultatie

PM

II. ARTIKELSGEWIJZE TOELICHTING

Artikel II (nieuw artikel 13)

Het eerste lid

[67] Vgl. artt. 139c en 273d WvSr.

Hiervoor wordt verwezen naar paragraaf 2 van het algemeen deel. In navolging van de staatscommissie Grondwet hebben wij ervoor gekozen om het recht en de daarop toegestane beperkingen in twee verschillende leden van artikel 13 op te nemen. Het betreft een wetgevingstechnische keuze, die niet leidt tot een verruiming van de toegestane beperkingen.

Het tweede lid

De staatscommissie Grondwet koos voor het gebruiken van de term machtiging in plaats van last, aangezien wetgeving verder geen onderscheid maakt tussen de in het huidige artikel 13 Grondwet gebruikte termen last en machtiging. De regering volgt de staatscommissie hierin en kiest voor de term machtiging.

De woorden 'een of meer bij de wet aangewezen ministers' laten toe dat de wet als eis stelt dat de machtiging moet worden verleend door meer dan één minister, bijvoorbeeld door twee of meer ministers gezamenlijk wanneer dat wenselijk zou zijn gelet op de verdeling van verantwoordelijkheden tussen ministers. Een voorbeeld daarvan zijn de artikelen 139a en 139c (oud) van het wetboek van Strafvordering, waarin besluitvorming van drie ministers werd vereist. De huidige wetgeving kent geen voorschriften die een machtiging eisen van meerdere ministers gezamenlijk. De Grondwet eist dat beperkingen in het belang van de nationale veiligheid in de gevallen bij de wet bepaald door of met machtiging van ten minste één minister plaatsvinden; dit kunnen er op grond van de wet ook meer zijn.

Het derde lid

Hiervoor wordt verwezen naar paragraaf 4 van het algemeen deel.

Artikel III (additioneel artikel)

Het onderhavige additionele artikel treft overgangsrecht. Het artikel biedt de gelegenheid om de wetgeving aan te passen aan de nieuwe eisen ten aanzien van beperkingen van het brief- en telecommunicatiegeheim, zoals die voortvloeien uit het voorgestelde nieuwe artikel 13. Het artikel bepaalt dat de bestaande beperkingen die in strijd zijn met het nieuwe artikel gedurende maximaal vier jaar in stand kunnen blijven, mits wordt voldaan aan het huidige artikel 13. Zoals is toegelicht in paragraaf 6 van het algemene gedeelte van deze toelichting, voorziet de huidige wetgeving voor het overgrote deel, ook met betrekking tot de nieuwe gebieden die onder de reikwijdte van artikel 13 vallen, reeds in de vereiste formeelwettelijke grondslag en de eis van een rechterlijke machtiging voor de beperkingen.