Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

33 989 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

Nr. 3 **MEMORIE VAN TOELICHTING**

I. ALGEMEEN 2

1. Inleiding 2
   - 1.1. Algemeen 2
   - 1.2. Achtergrond en noodzaak 2
   - 1.3. Doelstelling 6
   - 1.4. Consultatie 6
   - 1.5. Opzet van de memorie van toelichting 7

2. Inhoud en reikwijdte van het brief- en telecommunicatiegeheim 7
   - 2.1. De inhoud van het brief- en telecommunicatiegeheim 8
     - *2.1.1. Het rechtens te beschermen belang 8*
     - *2.1.2. Het brief- en telecommunicatiegeheim 9*
     - *2.1.3. De inhoud van de communicatie 11*
   - 2.2. De reikwijdte van het brief- en telecommunicatiegeheim 12
     - *2.2.1. Gebruik van communicatiemiddelen 12*
     - *2.2.2. De derde belast met het transport en/of opslag 13*
     - *2.2.3. Gerichtheid van de communicatie 15*
   - 2.3. Verkeersgegevens 17
   - 2.4. Toepassing van het communicatiegeheim in horizontale verhoudingen 20

3. Beperkingen 22
   - 3.1. Algemeen 22
   - 3.2. Rechterlijke machtiging 25
   - 3.3. Beperkingen in het belang van de nationale veiligheid 26

4. Verhouding tot internationale regelgeving 32
   - 4.1. Inleiding 32
   - 4.2. EU-recht 32
     - *4.2.1. Handvest van de grondrechten van de Europese Unie 32*
     - *4.2.2. Secundair EU-recht 33*
   - 4.3. Internationale verdragen 34

kst-33989-3
ISSN 0921 - 7371
's-Gravenhage 2014

5. Verhouding tot nationale wetgeving 36
5.1. Grondrechten 36
5.2. Strafrecht 37
5.3. Wet op de inlichtingen- en veiligheidsdiensten 2002 38
5.4. Algemene wet bestuursrecht 39
5.5. Telecommunicatiewet 40
5.6. Postwet 2009 42

6. Administratieve lasten en uitvoeringskosten 42

II. ARTIKELSGEWIJZE TOELICHTING 43

I. ALGEMEEN

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 meer 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 toenmalige kabinet oordeelde in reactie op het advies van de staatscommissie Grondwet dat de huidige techniekafhankelijke en limitatieve formulering van de beschermde communicatiemiddelen in de weg staat aan de normatieve betekenis van artikel 13 voor de wetgever en rechter. 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 de brief van de toenmalige Minister van Binnenlandse Zaken en Koninkrijksrelaties van 29 november 2011[2], waarover 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 en -technieken. 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. De nieuwe elektronische

[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.

wijze van communiceren heeft geleid tot ingrijpende wijzigingen in communicatiepatronen en informatiestromen in de samenleving. Stelden traditionele media zoals kranten, radio en televisie slechts enkelen in staat te communiceren met velen; de nieuwe elektronische communicatiemiddelen stellen velen in staat zelf informatie te zoeken en te distribueren. Waar de traditionele technologie voorzag in identieke informatie voor het gehele publiek, openen de nieuwe communicatietechnieken vele wegen voor velen om toegang te krijgen tot en het verspreiden van een vrijwel 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 gebruiken 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 diversificatie van communicatiemiddelen en -technieken – 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 en -technieken. 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, zodat de Grondwet recht doet aan deze nieuwe sociale, technische en culturele ontwikkelingen in de informatiemaatschappij.[5]
Het huidige artikel 13 beschermt het brief-, telefoon- en telegraafgeheim. Communicatie met behulp van technieken die gebruik maken van andere middelen wordt 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».[6] Indien het criterium is dat communicatie privé moet zijn, ongeacht het middel of de techniek met behulp waarvan wordt gecommuniceerd, is duidelijk dat andere elektronische vormen van communicatie niet langer onbesproken kunnen blijven. In deze zin sluit onderhavig voorstel aan bij hetgeen de grondwetgever in 1983 voor ogen had. De mate van bescherming die het huidige artikel 13 biedt, is afhankelijk van het gebruikte middel. Dat doet geen recht aan één van de belangrijkste kenmerken van de digitale samenleving, te weten conver-

---

[4] WRR-rapport *iOverheid* (2011), p. 32 e.v.
[5] Vgl. L.F. Asscher, *Communicatiegrondrechten*, Amsterdam: Otto Cramwinckel Uitgever 2002, p. 240.
[6] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 44.

gentie van communicatiemiddelen. Eén en hetzelfde communicatiemiddel wordt immers in toenemende mate gebruikt voor verschillende vormen van communicatie. Een voorbeeld is het verzenden van e-mail- en het gebruik van 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 gewijzigde omstandigheden in het gebruik van communicatiemiddelen voor diverse stromen van informatie is modernisering van artikel 13 noodzakelijk en dringend gewenst.

Bij de voorbereiding van het onderhavige voorstel zijn naast het rapport van de staatscommissie Grondwet ook eerdere adviezen, regeringsvoorstellen, alsmede 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[7], het daaropvolgende rapport van de Commissie Grondrechten in het Digitale Tijdperk (commissie-Franken)[8], de adviezen van de Raad van State naar aanleiding van de regeringsvoorstellen uit 2001[9], en de kritiek vanuit de wetenschap op de eerdere voorstellen. Vermeldenswaard is voorts 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.[10] Ten behoeve van het onderhavige wetsvoorstel hebben wij onderzoek laten verrichten naar de juridische en technische kwalificatie van verkeersgegevens, dat begin 2013 is opgeleverd.[11] In 2013 is eveneens het evaluatierapport van de Commissie Dessens dat ziet op de evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002 opgeleverd. De kabinetsreactie op dat rapport, alsmede de reactie van de Commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD) op dat rapport, volgden op 11 maart 2014.[12]

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[13] 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

---

[7] Kamerstukken II 1996/97, 25 443 nr. A.

[8] Rapport Grondrechten in het digitale tijdperk, Kamerstukken II 2000/01, 27 460, nr. 1, bijlage 1.

[9] 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).

[10] Kamerstukken II 2006/07, 27 460, nr. 5.

[11] J.M. Smits, Technische kwalificatie van verkeersgegevens ten behoeve van de herziening van artikel 13 Nederlandse Grondwet, februari 2013; B.J. Koops, Juridische kwalificatie van verkeersgegevens in het licht van artikel 13 Grondwet, februari 2013.

[12] Respectievelijk *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen* (Kamerstukken II 2013/14, 33 820, nr. 1), de kabinetsreactie op het rapport Commissie-Dessens (Kamerstukken II 2013/14, 33 820, nr. 2) en de reactie van de CTIVD op het rapport Commissie-Dessens van 11 maart 2014, kenmerk 2014/0046.

[13] Zie: *De grondwetsherziening 2006, Naar een nieuwe grondwet*. Documentatiereeks deel 39, SDU Uitgevers 2006, blz. 499–536 (artikel 13 Grondwet).

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.[14] 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.[15] In 2007 heeft het Europese Hof voor de Rechten van de Mens bepaald dat e-mail wordt beschermd onder artikel 8 EVRM, dat recht geeft op respect voor het privéleven en zijn correspondentie.[16]
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 die top zijn «freedom of expression and the free flow of information» erkend als «essential» voor de informatiesamenleving. In 2012 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. Dit standpunt werd recent bevestigd in een resolutie van de algemene vergadering van de VN getiteld «The right to privacy in the digital age.»[17] 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.[18] 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.[19] Tot slot wijzen wij op het belang van de wetgeving die in het kader van de Europese Unie tot stand is gebracht (zie paragraaf 4.2).

---

[14] CM (2005)56.
[15] 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.
[16] EHRM 3 april 2007, nr. 62617/00 (*Copland* t. *het Verenigd Koninkrijk*).
[17] Respectievelijk A/HRC/20/L/13, 5 juli 2012 en A/C.3/68/L.45, GA/11475, 18 december 2013.
[18] Kamerstukken II 1999/00, 27 460, nr. 1, blz. 11.
[19] *Overheden over internationalisering en ICT-recht*, C.J.C. Prins, E.J. Koops e.a., 2000, p. 85.

1.3. Doelstelling

Het voorstel vervangt de onschendbaarheid van het brief-, telefoon- en telegraafgeheim door het recht op eerbiediging van zijn brief- en telecommunicatiegeheim. Het heeft tot doel de huidige grondwettelijke bescherming die nu slechts 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 techniekonafhankelijke bescherming. De keuze voor een techniekonafhankelijke formulering is volgens ons de meest aangewezen wijze om de gewenste rechtsbescherming te garanderen van het rechtsbelang dat achter artikel 13 schuilgaat, namelijk het privé kunnen communiceren (zie paragraaf 2.1.1). Doordat niet langer enkel wordt gerefereerd aan specifieke communicatiemiddelen, maar naast een specifieke bescherming (briefgeheim) wordt gekozen voor een generieke bescherming (telecommunicatiegeheim) verkrijgen ook communicatie via e-mail, de sociale media en opslag van communicatie in de «cloud» (een door de aanbieder beheerd elektronisch netwerk waarnaar en waarin bestanden kunnen worden verzonden en opgeslagen) bescherming onder artikel 13. Het voorstel leidt daarmee tot 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 van communicatie gaat, in het tweede lid onder hetzelfde niveau van bescherming als nu voor het briefgeheim geldt. Beperking van het brief- en telecommunicatiegeheim is slechts mogelijk in de gevallen bij de wet bepaald, met een voorafgaande machtiging van de rechter. Indien de beperking plaatsvindt in het belang van de nationale veiligheid, is deze toegestaan in de gevallen bij de wet bepaald door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

1.4. Consultatie

Over een ontwerp van dit wetsvoorstel stond van 1 oktober 2012 tot 1 januari 2013 internetconsultatie open. Tegelijkertijd zijn enkele adviesorganen geconsulteerd over het conceptwetsvoorstel. Naast de algemene beoordeling van het wetsvoorstel zijn twee specifieke vragen gesteld tijdens de consultatie. Ten eerste zijn organisaties die worden geraakt door artikel 13, bijvoorbeeld omdat zij communicatie met een privékarakter inzien met het oog op een goede taakuitoefening, expliciet gevraagd hun zienswijze te geven op de gevolgen van dit voorstel voor hun werkwijze. Ten tweede is gevraagd of en om welke redenen er meerwaarde wordt gezien in de regelingsopdracht aan de wetgever in het voorgestelde derde lid en zo mogelijk voorbeelden te geven van onderwerpen die nader zouden moeten worden geregeld in wetgeving.
Over het conceptwetsvoorstel zijn adviezen ontvangen van de Vereniging van Nederlandse Gemeenten (VNG), het College van de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), het Nederlands Juristen Comité voor de Mensenrechten (NJCM), Privacy First, Bits of Freedom, het College voor de Rechten van de Mens (CRM), de Nederlandse Vereniging voor Rechtspraak (NVvR), het College van Procureurs-Generaal (OM) en het College bescherming persoonsgegevens (Cbp)[20]. Daarnaast zijn enkele uitvoeringsorganisaties gevraagd hun visie op het conceptwetsvoorstel te geven. Wij hebben de zienswijze ontvangen van de Belastingdienst, het Uitvoeringsinstituut werknemersverzekeringen, het Agentschap Telecom en de Nederlandsche Bank[21]. De

[20] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[21] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

internetconsultatie heeft buiten de eerder genoemde adviezen nog tien reacties opgeleverd, waarvan rekenschap is gegeven op betreffende onderdelen in de memorie van toelichting. De adviezen hebben op één punt geleid tot een wijziging van de tekst van het wetsvoorstel en op een groot aantal punten tot verduidelijkingen en aanvullingen in de tekst van de memorie van toelichting. In de wettekst is de formulering van de beperkingsclausule in het tweede lid aangepast voor zover het beperkingen in het belang van de nationale veiligheid betreft (zie par. 3.3). Een grote meerderheid van de geconsulteerde organisaties heeft waardering voor het initiatief tot wijziging van artikel 13, hetgeen vaak als dringend noodzakelijk wordt aangemerkt. Er is erkenning voor de constatering dat artikel 13 aan modernisering toe is. Voorts zijn de adviezen overwegend positief over het gekozen object van bescherming: het brief- en telecommunicatiegeheim. De adviezen bevatten voornamelijk opmerkingen die om duiding of nadere uitwerking van het begrippenkader en de reikwijdte van het voorgestelde artikel 13 vragen. Hieraan is tegemoet gekomen door de memorie van toelichting op de betreffende onderdelen aan te vullen. Daarnaast is op een aantal meer fundamentele punten geadviseerd het voorstel aan te passen, in het bijzonder betreffende de duur van de bescherming van het brief- en telecommunicatiegeheim door artikel 13, mede in relatie tot de andere privacygrondrechten, de bevoegde instantie die een machtiging kan afgeven voor beperkingen van het brief- en telecommunicatiegeheim in het belang van de nationale veiligheid, alsmede onafhankelijke controle daarop, de bescherming van verkeersgegevens onder artikel 13 en de opname van een grondwettelijke notificatieplicht. Ook op deze punten is nader ingegaan in de betreffende paragrafen van de toelichting, waarin wij motiveren welke afweging wij hebben gemaakt en waarom. De adviezen van de NVvR, het OM en de uitvoeringsorganisaties duiden niet op grote knelpunten voor de uitvoeringspraktijk. Wel is nadere aandacht gevraagd voor de gevolgen van de eis van een rechterlijke machtiging voor toezichthouders in de zin van de Algemene wet bestuursrecht en de belastingheffing, waarop is ingegaan in paragraaf 5.4. Het CRM en Cbp hebben in hun adviezen tevens aandacht gevraagd voor een herbezinning op andere grondrechten in relatie tot het digitale tijdperk, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer (artikel 10 Grondwet). Aan de onderlinge verhouding tussen deze grondrechten is nadere aandacht besteed in paragraaf 5.1.

1.5. Opzet van de memorie van toelichting

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 door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Een plaatsbepaling van het voorgestelde artikel 13 tegen de achtergrond van relevante internationale regelgeving, alsook de relatie met nationale wetgeving worden tot slot uitgewerkt in de paragrafen 4 en 5.

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 via deze middelen 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, welke in beheer is van een (private) derde. De overheid neemt vrijwel nooit meer het transport van communicatie voor haar rekening, maar dat neemt niet weg dat artikel 13 de burger behoort te beschermen tegen heimelijke overheidsinzage van privé-communicatie, die door een derde, niet zijnde de verzender of ontvanger, wordt getransporteerd en/of opgeslagen. Voor zover in de toelichting wordt gesproken over bescherming tegen inzage in privé-communicatie door de derde die de communicatie transporteert en/of opslaat, volgt die bescherming uit de lagere wetgeving en niet uit de Grondwet als zodanig. Dergelijke wettelijke bepalingen zijn een weerslag van het rechtens te beschermen belang dat ten grondslag ligt aan het brief- en telecommunicatiegeheim.

2.1. De inhoud van het brief- en telecommunicatiegeheim

2.1.1. 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 vertrouwelijkheid van communicatie vormt in een democratische rechtsstaat een zwaarwegend belang. De staatscommissie Grondwet omschreef het belang van artikel 13 als «men moet in een democratische samenleving vertrouwelijk met elkaar kunnen communiceren, zonder de angst dat de overheid meeluistert.»[22] Dit rechtens te beschermen belang achter het huidige artikel 13, is gelijk aan het rechtens te beschermen belang achter het brief- en telecommunicatiegeheim in het onderhavige wetsvoorstel. Alle gerichte communicatie die aan een derde wordt toevertrouwd ten behoeve van het transport en/of opslag, geniet bescherming van artikel 13. Het feit dat de verzender (een deel van de) controle over de communicatie uit handen geeft aan de derde, maakt dat additionele bescherming van de inhoud van die communicatie is aangewezen.

Met privé-communicatie wordt bedoeld communicatie die niet voor het publiek toegankelijk is. Het betreft informatie die geheim is tussen verzender en ontvanger; anderen mogen daarvan geen kennisnemen zonder toestemming van de verzender of ontvanger. Het gaat aldus om niet-openbare communicatie. Openbare communicatie, zoals het plaatsen van een «tweet» waarvan de zichtbaarheid niet is beperkt tot zogenoemde «volgers» van de auteur (niet afgeschermd), of een «blog» op een website, wordt beschermd door het recht op vrijheid van meningsuiting, dat is vastgelegd in artikel 7 van de Grondwet. Die bepaling geeft het recht om vrij informatie te openbaren (en op basis van artikel 10 EVRM te vergaren) en wordt daarom ook wel aangeduid met de term communicatie*vrijheid*. Privé-communicatie is daarvan te onderscheiden en vormt het spiegelbeeld van de communicatievrijheid, omdat het juist ziet op het besloten houden van de informatie: het communicatie*geheim*.

Veelal wordt privé-communicatie gezien als één specifiek aspect van de persoonlijke levenssfeer, dat vanwege de mogelijkheid tot heimelijke inzage bijzondere bescherming rechtvaardigt. Artikel 10 Grondwet biedt onvoldoende bescherming aan privé-communicatie. Voor doorbreking van het brief- en telecommunicatiegeheim achten wij – anders dan bij een beperking van de persoonlijke levenssfeer (artikel 10 Grondwet) – vanwege de heimelijkheid van de inzage door de overheid in beginsel een rechterlijke machtiging noodzakelijk. Rechtvaardiging voor deze extra bescherming onder artikel 13 ten opzichte van artikel 10, dat een dergelijk specifiek competentiecriterium niet vastlegt, is gelegen in het feit dat inbreuken op het brief- en telecommunicatiegeheim naar hun aard vrijwel

[22] Rapport staatscommissie Grondwet 2010, p. 85.

nooit worden opgemerkt door de verzender of ontvanger. Dat heimelijke aspect, doordat het een vordering tot inzage van communicatie bij *een derde* betreft, maakt het brief- en communicatiegeheim kwetsbaar. Burgers behoren te kunnen communiceren vanuit de gedachte dat zij onbelemmerd van gedachten kunnen wisselen, gevoelens kunnen uitwisselen, informatie kunnen vergaren of gericht informatie kunnen verspreiden met behulp van communicatiemiddelen, zonder daarbij op onrechtmatige wijze heimelijk te worden gadegeslagen door de overheid. Burgers kunnen immers alleen dan privé communiceren indien zij niet bevreesd hoeven zijn voor heimelijke inzage. De kwetsbaarheid van de inhoud van de communicatie vanwege de feitelijke toegang door de derde belast met 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.

2.1.2. Het brief- en telecommunicatiegeheim

Alle vormen van telecommunicatie en de communicatie per brief verdienen naar ons oordeel bescherming onder artikel 13. De brief wordt in het eerste lid separaat genoemd omdat in de verschijningsvorm van dit communicatiemiddel geen sprake is van een elektronische toepassing zonder dat iets of iemand zich fysiek verplaatst. Artikel 2, eerste lid, onder a, van de Postwet 2009 verstaat onder een brief «de op een fysieke drager aangebrachte geadresseerde schriftelijke mededelingen», welke definitie deels is ontleend aan de Postrichtlijn[23] (artikel 2, onder 7). Een brief kan zowel verpakt zijn (in een envelop) als niet verpakt (een ansichtkaart). Ook geadresseerd drukwerk valt eronder. In de Postwet 2009 is er sprake van een brief zodra een poststuk geadresseerd is en een mededeling bevat in welke vorm dan ook, ongeacht of het een standaardmededeling is of niet.[24] De definitie in de Postwet 2009, alsook de bestaande interpretatie van het begrip brief in het huidige artikel 13 Grondwet, zijn leidend voor de uitleg van het begrip «brief» in het voorgestelde nieuwe artikel 13. Telecommunicatie, een samenstelling van het Griekse «tèle» ofwel ver en het Latijnse «communicare» ofwel mededelen, betekent letterlijk genomen het overbrengen van informatie over grote afstand zonder dat iets of iemand zich fysiek verplaatst. Die overdracht van informatie geschiedt via communicatiekanalen met behulp van kabels of elektromagnetische velden. Wat betreft de verhouding van de grondwettelijke definitie van het begrip telecommunicatie tot datzelfde begrip in lagere regelgeving valt het volgende op te merken. 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 begrip telecommunicatie in de zin van artikel 13 is ruimer 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 ontwik-

---

[23] Richtlijn 97/67/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende gemeenschappelijke regels voor de ontwikkeling van de interne markt voor postdiensten in de Gemeenschap en de verbetering van de kwaliteit van de dienst, PbEU 1998, L 15, zoals deze laatstelijk is gewijzigd bij Richtlijn 2008/6 van het Europees Parlement en de Raad van 20 februari 2008, PbEU 2008, L 52.

[24] Kamerstukken II 2005/06, 30 536, nr. 3, blz. 31.

kelen (niet-elektronische) communicatiemiddelen. Een dergelijke techniekafhankelijke interpretatie achten wij niet opportuun voor de Grondwet met het oog op mogelijke technologische ontwikkelingen en toepassingen in de communicatietechniek in de verre toekomst. Hoewel dit naar de huidige stand van de wetenschap niet waarschijnlijk is, kan immers niet worden uitgesloten dat in de toekomst ook niet-elektronische communicatiemiddelen 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» in de Grondwet dan thans gebruikelijk is in het kader van de genoemde wettelijke regelingen. Het begrip «telecommunicatie» in de zin van artikel 13 omvat uiteraard alle vormen van telecommunicatie zoals die in de bestaande juridische kaders worden gebruikt. Het is daarmee dus niet in tegenspraak, maar ruimer. Het begrip telecommunicatie omvat mede de communicatiemiddelen telefoon en telegraaf uit het huidige artikel 13.

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 door een derde; telecommunicatie omvat in dit verband ook opslag van informatie door een derde voorafgaand, tussentijds of na afloop van het transport van de betreffende communicatie. 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 webmaildienst.

Aan de bescherming van de transportfase en van de (tussentijdse) opslag van communicatie ligt de overweging ten grondslag dat hierbij een derde betrokken is, waardoor de verzender geen exclusieve controle heeft over het bericht. De derde die de overdracht en/of opslag van de inhoud van de communicatie beheert, kan de communicatie zonder medeweten van de verzender inzien en doorgeven aan anderen, waaronder de overheid. Tegen deze kwetsbaarheid wil het brief- en telecommunicatiegeheim aldus een dam opwerpen. De tweede overweging bij 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 communicatie*middel* 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 «brief- en telecommunicatiegeheim» uitgebreid naar alle huidige en toekomstige communicatiemiddelen. De begrippen brief en telecommunicatie vormen elkaars complement, waarmee tezamen alle denkbare vormen van communicatie worden aangeduid en beschermd onder artikel 13.

Het onderscheid tussen brief en telecommunicatie is daarbij niet langer van betekenis voor de mate van rechtsbescherming die aan de betreffende communicatie toekomt onder artikel 13. Onder het huidige artikel 13 is rechterlijke toestemming vereist voor kennisname van de inhoud van de brief bij degene die is belast met het transport daarvan, ook indien inzage wordt verlangd op grond van de nationale veiligheid. Bij het telefoongesprek en telegraafberichten is voor kennisneming van de inhoud toestemming van de Minister steeds voldoende. Het wetsvoorstel zal de bescherming van de telecommunicatiemiddelen aldus optrekken naar het niveau van de brief: rechterlijke toestemming is vereist, behalve wanneer inzage wordt verlangd in het belang van de nationale veiligheid. Thans is op wettelijk niveau vastgelegd dat ingevolge het huidige artikel 13 Grondwet de brief in het belang van de nationale veiligheid enkel kan worden ingezien met toestemming van de rechter. Het voorgestelde artikel 13 laat ruimte om dit laatste te handhaven.

In het voorstel wordt de bescherming van alle middelen gelijkgetrokken; er wordt niet langer een onderscheid in beschermingsniveau gemaakt tussen de brief enerzijds en de andere communicatiemiddelen anderzijds. Een belangrijke doelstelling van het wetsvoorstel is het techniekonafhankelijk maken van artikel 13. Het bepleiten van een uitzonderingspositie voor één middel, de brief, vinden wij in dat licht niet overtuigend. Het argument van traditie is gelet op de convergentie van communicatiemiddelen onvoldoende. Aan het separaat benoemen van de communicatiemiddelen staat het gelijktrekken van het beschermingsniveau niet in de weg. Hetgeen beschermd dient te worden is immers de inhoud van het bericht. Het maakt daarbij – vanwege de convergentie van communicatiemiddelen – niet langer uit met welk middel de inhoud van de communicatie wordt verstuurd.[25] Het verschillend beschermen op basis van het middel leidt tot een techniekafhankelijke benadering in de mate van bescherming. Gelet op het feit dat de inhoud de essentie is van het te beschermen object van artikel 13 en het gegeven dat de andere communicatiemiddelen een belangrijke plaats in het maatschappelijk leven hebben verworven, dient de overheid zich te onthouden van een voorkeur voor een hogere bescherming van het ene of het andere middel. In dit licht is het onderscheid in bescherming tussen briefvervoer en transport via de andere middelen arbitrair. Met de gekozen benadering wordt bovendien voorkomen dat later over nu nog onbekende middelen op grondwettelijk niveau moet worden beslist welke mate van bescherming zij zullen genieten.[26] Voor het overige merken wij op dat voor zover een onderscheid in het verleden wel werd gerechtvaardigd op grond van de mate van geslotenheid (enveloppe) of openheid (telefoonkabel of telegraaf) van het middel, dit onderscheid gelet op de convergentie van middelen niet langer maatgevend kan zijn voor het beschermingsniveau. Het gesloten karakter is niet meer voorbehouden aan de brief; beslotenheid kan bijvoorbeeld ook in elektronische middelen worden aangebracht (bijvoorbeeld met behulp van encryptie bij een e-mailbericht).

2.1.3. De inhoud van de communicatie

Communicatie betekent uitwisseling van informatie van welke aard en in welke vorm dan ook tussen een verzender en een of meer ontvangers. In deze toelichting wordt op diverse plaatsen het begrip «bericht» gebruikt als een veel voorkomende vorm van communicatie. Te denken valt bijvoorbeeld aan een e-mailbericht of een sms-bericht. Ook de uitwisseling van informatie met een computer van een instantie valt onder communicatie. Er is sprake van communicatie in de zin van artikel 13 als er uitwisseling plaatsvindt van informatie, gevoelens en/of gedachten via een middel beheerd door een derde. Of die ander een persoon is of een apparaat dat vervangend is voor een persoon of een instantie, is niet van belang. Het gaat erom dat er interactie is tussen twee of meer partijen. Het enkele invoeren van gegevens voor eigen gebruik in de computer is nog geen communicatie, omdat er geen derde is die deze gegevens beheert.[27] Dat sprake is van communicatie moet blijken uit een actie, welke zichtbaar is voor de transporteur van de communicatie. Daarvan kan bijvoorbeeld al sprake zijn bij de opslag van een conceptbericht in een webmailbox. Zolang de derde nog geen beheer heeft over het bericht valt de te transporteren communicatie buiten de bescherming van artikel 13. Dat betekent dat een conceptbericht dat is opgeslagen in een webmailbox wordt beschermd door artikel 13, terwijl een conceptbericht dat is opgeslagen op de harde schijf van een computer niet valt onder de

---

[25] L. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving* (diss.), UvA 2002, p. 104.

[26] Idem, p. 235.

[27] Vgl. artikel 126l Wetboek van Strafvordering, Kamerstukken II 1996/97, 25 403, nr. 3, blz. 36.

bescherming van artikel 13. Het begrip inhoud van communicatie dient in dit kader ruim te worden opgevat; daaronder worden onder meer begrepen gevoelens, gedachten, gegevens en (feitelijke) informatie of bestanden die wordt overgedragen. De inhoud van brief- en telecommunicatie kan zowel tekst als beelden bevatten, maar ook muziek kan deel uitmaken van de inhoud van de communicatie. De gekozen vorm om een boodschap te communiceren is evenmin als het gekozen transportmiddel bepalend.
Voor de toepassing van artikel 13 maakt het geen verschil of het communicatie van persoonlijke of zakelijke aard betreft. Een ieder heeft er in een democratische samenleving belang bij dat het geheim van zowel zakelijke communicatie als persoonlijke communicatie gerespecteerd wordt, conform het adagium «geen boodschap aan de boodschap». Dus ook zakelijke communicatie die in beheer is bij een derde, maar niet voor die derde is bestemd of van hem afkomstig is, valt onder de bescherming van artikel 13.
Van belang bij het beantwoorden van de vraag of het gaat om de *inhoud* van communicatie zijn die aspecten – veelal de in het bericht geuite informatie, gevoelens en gedachten – van de communicatie waarvoor de verzender verantwoordelijk is. Deze inhoud van de communicatie is te onderscheiden van andere gegevens die tijdens het communicatieproces die worden gegenereerd met betrekking tot de totstandkoming, de duur en het tijdstip van de communicatie. Voor die gegevens zijn anderen – veelal de derde die het bericht transporteert of opslaat – verantwoordelijk en geldt een ander beschermingsregime. De bescherming van artikel 13 ziet enkel op de inhoud van de communicatie die de verzender wenst over te brengen naar één of meer ontvangers. De bescherming van de andere gegevens die gaandeweg in het communicatieproces worden gegenereerd worden, voor zover het persoonsgegevens betreft, beschermd onder artikel 10 van de Grondwet. De inhoud van de communicatie is aldus te onderscheiden van de zogenoemde verkeersgegevens. Deze 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 is, gelden drie cumulatieve criteria, te weten het gebruik van een communicatiemiddel, het toevertrouwen van de communicatie aan een derde die is belast met het transport en/of opslag daarvan en tot slot de noodzaak van de gerichtheid van de communicatie. Deze drie criteria worden hierna verder uitgewerkt.

2.2.1. Gebruik van communicatiemiddelen

In het licht van 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 een bericht dat ter verzending en bezorging bij de ontvanger aan de zorg van een derde is toevertrouwd (voorheen doorgaans een overheidsinstelling) ook daadwerkelijk wordt verzonden en bezorgd zonder dat de overheid 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».[28] Deze zinsnede is in 1983 geschrapt om te bereiken dat het briefgeheim zich ook zou uitstrekken tot andere overheidsinstellingen, zoals gevangenisdirecties, die evenzeer moeten voldoen aan de eisen van artikel 13 voor zover geen verdergaande beperkingen zijn toegestaan op grond van artikel 15, vierde lid, Grondwet.[29] 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 de overheid.
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 het transport van de communicatie tot stand wordt gebracht. In paragraaf 2.1.2 is toegelicht welke middelen onder de begrippen brief en telecommunicatie kunnen worden geschaard. Deze omvatten uiteraard de in het huidige artikel 13 opgesomde communicatiemiddelen. Gelet op deze eis valt het gewone mondelinge gesprek («live-gesprek») niet onder de bescherming van artikel 13.
Welke de aard is van het communicatiemiddel doet 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.

2.2.2. De derde belast met het transport en/of opslag
Als tweede criterium voor de toepasselijkheid van artikel 13 geldt dat communicatie is toevertrouwd aan een derde ten behoeve van het transporteren en/of opslaan daarvan. Dit criterium is analoog aan de uitleg van het huidige artikel 13, eerste lid. Men moet erop kunnen vertrouwen dat aan een derde toevertrouwde communicatie op de bestemde plaats wordt bezorgd zonder dat de overheid kennis kan 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 die voor eenieder toegankelijk is). Dit impliceert dat de bescherming geldt voor zover en zolang de inhoud van communicatie aan een derde voor de overdracht en/of opslag is toevertrouwd. Iedere aanbieder van een communicatiedienst (aan het publiek) moet worden beschouwd als derde in de zin van artikel 13. Hieronder kunnen in ieder geval alle aanbieders worden gerekend in de zin van de Telecommunicatiewet en de Postwet 2009, zoals aanbieders van (openbare) elektronische communicatiediensten en postvervoerbedrijven. De reikwijdte van artikel 13 beperkt zich evenwel niet tot aanbieders van communicatiediensten in de zin van deze specifieke regelgeving. Ook aanbieders van niet-openbare telecommunicatiediensten, zoals bedrijfsnetwerken, en aanbieders van private koeriersdiensten vallen onder de reikwijdte van artikel 13, voor zover zij communicatie transporteren en/of opslaan. Wel dient op enig moment in het proces sprake te zijn van transport van communicatie. Dat betekent dat de overheid zonder de grondwettelijk vereiste machtiging geen inzage mag vorderen van communicatie die is of wordt getransporteerd door aanbieders van besloten elektronische communicatiediensten, zoals bedrijfsnetwerken.

---

[28] 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.
[29] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 44.

Deze verticale werking van artikel 13 Grondwet, staat los van de geldende afspraken in private verhoudingen tussen de aanbieder en afnemer van de betreffende dienst bij gebruikmaking van een besloten communicatienetwerk. Zo kan een werkgever bijvoorbeeld onder bepaalde omstandigheden communicatie die is verzonden door de werknemer inzien, zonder een machtiging van een rechter.
Thans wordt de duur van de bescherming van artikel 13 bepaald door de zogenoemde «transportfase», die in het fysieke communicatieproces nog helder af te bakenen is tot aan de ontvangst van het bericht. Zodra de brief door de postbode wordt afgeleverd en de betreffende brief op de deurmat valt, houdt de betrokkenheid van de derde in het communicatieproces op en mitsdien ook de bescherming van artikel 13.[30] Bij gebruik van elektronische communicatiemiddelen loopt de «transportfase» veelal over in de opslag van het bericht in de conceptfase en bewaring van het bericht na afloop van het transport, omdat op die momenten de derde, die is belast met het transport, ook het beheer heeft over de opslag van het bericht. In die hoedanigheid is deze derde in deze situatie feitelijk in de gelegenheid kennis te nemen van de inhoud van het bericht. De vraag rijst of de overheid in de situatie van het transport of de opslag van het bericht bij de derde inzage zou kunnen vorderen van berichten – wanneer ze nog in concept in bijvoorbeeld de persoonlijke webmail *inbox* zijn opgeslagen (het bericht bevindt zich in het beheer van de communicatiedienstverlener), of wanneer het bericht is gelezen en opgeslagen blijft in de webmail *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).
De technologische werkelijkheid, waarin transport en opslag van communicatie in elkaar over lopen, dient te worden vertaald in de reikwijdte van het brief- en telecommunicatiegeheim, omdat de bescherming heeft te gelden zolang de derde feitelijk toegang heeft tot de inhoud van de communicatie en de overheid in het verlengde daarvan bij deze derde inzage zou kunnen vorderen in de communicatie. Onder deze omstandigheden is de privé-communicatie immers kwetsbaar.
Maatgevend is dat zolang de derde de communicatie beheert en toegang heeft tot de inhoud, de bescherming van het brief- en telecommunicatiegeheim dient te gelden. Dit 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 via sociale media – en dat de overheid uitsluitend via de derde kennis mag nemen van de inhoud van het bericht met inachtneming van de eisen van artikel 13. De bescherming onder artikel 13 houdt dus niet op na afloop van de transportfase, zoals het geval is in de huidige interpretatie van de kanaalbescherming onder artikel 13. Zolang een derde toegang heeft tot de communicatie geniet deze bescherming onder het voorgestelde artikel 13. De betreffende bescherming is niet begrensd in de tijd en beslaat zowel tussentijdse opslag van communicatie door een derde als opslag voorafgaand aan of na afloop van de transportfase.
Uit het criterium dat het moet gaan om communicatie die is toevertrouwd aan een derde ten behoeve van het transporteren daarvan, volgt dat het moet gaan om communicatie die niet voor die derde is bestemd of van hem afkomstig is. Met andere woorden: de derde voert slechts het beheer over het transport en/of opslag van communicatie tussen de verzender en de ontvanger(s) daarvan. Het op basis van wettelijke bevoegdheden vorderen van de inhoud van communicatie bij de verzender of de

[30] HR 18 oktober 1994, NJ 1995, 101, ro. 9.3. De bescherming van artikel 13, eerste lid, Grondwet strekt zich niet uit tot een door looninspecteurs van een bedrijfsvereniging (en aan het FIOD ter beschikking gestelde) in beslag genomen administratie uit de woning en het kantoor van verdachte.

ontvanger zelf, valt niet onder de reikwijdte van artikel 13, omdat inzage dan niet buiten de betrokken partijen om gaat.
In het leeuwendeel van de gevallen is de derde die de overdracht en eventueel opslag verzorgt niet de overheid, maar een private partij. Ook de derde in de hoedanigheid van private partij het transport en eventueel opslag verzorgt, mag niet zonder toestemming van de verzender kennisnemen van het bericht. Deze bescherming is nu reeds grotendeels 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 voor zover het gaat om aanbieders van postvervoerdiensten en de artikelen 11.2a en 18.13 lid 2 Telecommunicatiewet voor zover het gaat om aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten). Op de werking van het brief- en communicatiegeheim in horizontale verhoudingen wordt nader ingegaan in paragraaf 2.4.
Uitgaand van het vereiste van de aanwezigheid van een communicatiemiddel en de derde die het transport van communicatie 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 niet beschermd door artikel 13, omdat geen gebruik wordt gemaakt van een communicatiemiddel, noch een derde is betrokken bij de overdracht van de inhoud van de communicatie. Het *live-gesprek* is echter niet onbeschermd. Vindt het *live-gesprek* plaats in de openbare ruimte, dan valt dit onder de bescherming van artikel 10 Grondwet. 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 brief- en telecommunicatiegeheim wordt de inhoud van de communicatie aan een derde toevertrouwd, waarmee de controle daarover uit handen wordt gegeven en inzage heimelijk geschiedt zonder dat de verzender, die verantwoordelijk is voor de inhoud van de communicatie, daar weet van zal hebben. 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 het transport en/of de opslag van het bericht. Als een derde een andere partij inschakelt voor het verrichten van bepaalde werkzaamheden, waardoor de feitelijke beschikkingsmacht kan verschuiven, maar de juridische beschikkingsmacht blijft bestaan, blijft deze verantwoordelijk voor de dienstverlening en de naleving van de wettelijke verplichtingen.[31] Dat geldt ook voor de naleving van het brief- en telecommunicatiegeheim. Daaraan doet niet af dat wellicht op enig moment ook de ontvanger 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 het risico op heimelijke inzage aanwezig en is bescherming aangewezen.

2.2.3. 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 (zie ook par. 2.1.3 over het begrip communicatie). Dit is het derde criterium waaraan moet zijn voldaan, wil artikel 13 van toepassing zijn. In het communicatieverkeer is steeds vast te stellen of

[31] Zie HvJ EU 22 november 2012 en artikel 11.2a Tw.

communicatie gericht is, hetgeen dit criterium een noodzakelijke en bruikbare mate van objectiveerbaarheid verleent. Artikel 11.1, onder e, van de Telecommunicatiewet omschrijft «communicatie» als informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen. Er bestaat geen maximum aantal ontvangers in absolute termen om te bepalen wanneer gerichte communicatie overgaat in ongerichte communicatie. De geadresseerden – hoezeer ook velen in getal – zijn immers nog altijd individueel herleidbaar. Het aantal ontvangers vormt geen onderscheidend criterium. Niet alleen de brief, de e-mail of het bericht dat via een *sociaal medium* aan een aantal ontvangers wordt verstuurd, vallen onder de reikwijdte van artikel 13, maar ook gerichte reclame-uitingen 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 meer afzonderlijk te bepalen ontvangers op het moment van verzending. Denkbaar is dat de verzender iets aan zichzelf adresseert, bijvoorbeeld door zichzelf te mailen (al dan niet naar een ander e-mailadres), dat de verzender een bericht «deelt» met een af te bakenen groep personen via sociale media, of communicatie opslaat 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 ontvangers.

De eis van gerichtheid van de communicatie is niet anders dan onder het huidige artikel 13.[32] Onder het huidige artikel 13 wordt bijvoorbeeld ook een gelijktijdig aan alle leden van een vereniging verzonden nieuwsbrief door het grondrecht beschermd. 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 – én van – organisaties, instellingen en andere entiteiten. Tegenwoordig wordt veel van apparaat naar apparaat gecommuniceerd, terwijl de persoon achter de verzender en ontvanger wellicht niet direct kenbaar zijn. Ook dan is sprake van gerichte communicatie

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 zijn vormen van gerichte communicatie. De gerichtheid 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 plaatsen van een niet-afgeschermd bericht op een sociaal medium 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 in de openbaarheid wil brengen. In

[32] Hoge Raad 29 maart 1994, D&D 1994, p. 314.

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.
De gerichtheid van de communicatie is 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. Dit wisselende gebruik van communicatietechnieken voor zowel massacommunicatie als besloten communicatie werd hiervoor reeds geduid met het begrip «convergentie».[33] Genoemde afbakening van het brief- en telecommunicatiegeheim is noodzakelijk om te voorkomen dat het toepassingsbereik ervan onverantwoord ruim wordt. De inhoud van ongerichte communicatie valt buiten het bereik van artikel 13.

2.3. Verkeersgegevens

Bij communicatie met gebruikmaking van daartoe bestemde kanalen ontstaan gegevens die niet zien op de gecommuniceerde boodschap als zodanig (de inhoud), maar gegevens die betrekking hebben op de overdracht of op de opslag van de communicatie, die inzicht kunnen geven in communicatiepatronen.[34] Te denken valt bijvoorbeeld aan 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» of «metadata». Opgemerkt zij dat «verkeersgegevens» in diverse wetten op verschillende wijzen worden gedefinieerd. In de EU-richtlijnen die zien op elektronische communicatienetwerken en -diensten[35] worden verkeersgegevens omschreven als die gegevens, die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan. Artikel 11.1 sub b van de Telecommunicatiewet volgt deze definitie als gevolg van implementatie. 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». Artikel 28 Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) kent vergelijkbare bewoordingen. Verkeersgegevens worden ook wel «inhoudloze transmissiegegevens» genoemd.[36]

---

[33] 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.
[34] Zie ook Rapport staatscommissie Grondwet 2010, p. 89.
[35] Artikel 5, eerste lid, van de ePrivacyrichtlijn (Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juni 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEG* 2002, L 201).
[36] A.H.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen 2006, p. 4–5.

Uit de jurisprudentie van het EHRM volgt dat verkeersgegevens vallen onder de reikwijdte van artikel 8 EVRM.[37] Als deze gegevens worden gebruikt, bijvoorbeeld voor het opmaken van een telefoonrekening of in het kader van de opsporing, moet daarbij dus aan de eisen uit artikel 8, tweede lid, zijn voldaan. In de literatuur over deze jurisprudentie wordt doorgaans betoogd dat verkeersgegevens een integraal onderdeel uitmaken van het correspondentiegeheim.[38]Het Hof heeft in de zaak *Malone* bepaald dat: «By its very nature, metering is (...) to be distinguished from interception of communications (...). The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to *an issue under Art. 8*. The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts (...) to an interference with a right guaranteed by Art. 8.» Deze lijn bevestigde het Hof in P.G. en J.H.: «It is not in dispute that the obtaining by the police of information relating to the numbers called on the telephone in B.'s flat interfered with the private lives *or* correspondence (in the sense of telephone communications) of the applicants who made use of the telephone in the flat or were telephoned from the flat.» Het EHRM laat in deze rechtsoverwegingen in het midden of verkeersgegevens onder het algemene recht op respect voor het privéleven vallen dan wel onder het correspondentiegeheim van artikel 8 EVRM. Er valt slechts vast te stellen dat het verwerken van verkeersgegevens moet voldoen aan de eisen die artikel 8 EVRM daaraan stelt. De jurisprudentie van het EHRM dwingt de grondwetgever niet om aan het gebruik van verkeersgegevens dezelfde eisen te stellen als aan een inbreuk op het geheim van de inhoud van communicatie. Ook het EU-Handvest van de Grondrechten is inmiddels door het Hof van Justitie in verband gebracht met bewaring van verkeersgegevens als bedoeld in de richtlijn dataretentie; hierbij kunnen volgens het Hof de artikelen 7 (eerbiediging van het privéleven, het familie- en gezinsleven, de woning en communicatie) en 8 (bescherming van persoonsgegevens) in beeld komen.[39] Hierop wordt nader ingegaan in par. 4.2.2 van deze toelichting. Verkeersgegevens zijn van groot belang voor de opsporing van cyberaanvallen, of voor het gebruik van firewalls en spamfilters, omdat zij patronen in datastromen blootleggen. Wij maken in dit voorstel een onderscheid tussen enerzijds klassieke verkeersgegevens, die geen inhoud van communicatie betreffen, en anderzijds gegevens die technisch gezien weliswaar als verkeersgegevens worden aangemerkt, maar niettemin betrekking hebben op de inhoud van communicatie. De verkeersgegevens die in de wetgeving, in het bijzonder het Wetboek van Strafvordering, de Telecommunicatiewet en in de Wiv 2002 zijn aangemerkt als verkeersgegevens, genieten geen bescherming van artikel 13. Het betreft immers geen gegevens die de inhoud van communicatie betreffen. Voor zover verkeersgegevens tevens persoonsgegevens zijn, genieten deze gegevens in de huidige situatie wel de bescherming van artikel 10 Grondwet, de Wet bescherming persoonsgegevens (Wbp) en van de Wiv 2002. Verkeersgegevens kunnen naar hun aard raken aan de (tele)communicatie*vrijheid*. De Raad van State merkte ter zake van verkeersgegevens in zijn advies op het wetsvoorstel uit 2001 op: «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

---

[37] EHRM 2 augustus 1984, NJ 1988, 534 (*Malone* t. *het Verenigd Koninkrijk*); EHRM 25 september 2001, NJ 2003, 670 (P.G. en J.H. t. het Verenigd Koninkrijk).

[38] Bijv. Dommering in zijn annotatie bij *P.G. en J.H.* t. *het Verenigd Koninkrijk*, NJ 2003, 670, onder 2.

[39] Zie ook *Digital Rights* t. *Ierland en Kärntener Landesregierung t. Seitlinger*, HvJ EU, C-293/12 en C-594/12 van 8 april 2014.

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.»[40] De Commissie Franken en de meerderheid van de staatscommissie Grondwet wilden verkeersgegevens niet binnen de reikwijdte van artikel 13 brengen.[41] Over de vraag of verkeersgegevens onder de reikwijdte van artikel 13 moeten worden geschaard is in de loop der tijd uiteenlopend geadviseerd. Enerzijds wordt verwezen naar de jurisprudentie van artikel 8 EVRM dat verkeersgegevens onder de reikwijdte van die bepaling brengt, anderzijds wordt betoogd dat geen ruimere betekenis aan de definitie van verkeersgegevens moet worden toegekend dan juridisch en technisch gebruikelijk is.
Wij zijn net als het toenmalige kabinet en de staatscommissie Grondwet van mening dat er onvoldoende rechtvaardiging is om aan alle verkeersgegevens hetzelfde niveau van grondwettelijke bescherming te geven als aan de communicatie-inhoud zelf.[42] Bij het gebruik van moderne communicatiemiddelen ontstaan talrijke verkeersgegevens. Deze gegevens leggen aanzienlijk meer informatie bloot over de communicatie van personen dan in de analoge wereld. Verkeersgegevens kunnen raken aan de persoonlijke levenssfeer van personen en het is evident dat ze in zoverre bescherming moeten genieten. Bezien vanuit het hiervoor beschreven rechtens te beschermen belang vallen verkeersgegevens in beginsel niet onder de reikwijdte van het voorgestelde artikel 13. Voor verkeersgegevens kan gelet op de aard van deze gegevens – te weten gegevens die informatie verschaffen omtrent het communicatieproces en voor zover zij niet de inhoud van de communicatie betreffen – het beperkingsregime van artikel 10 Grondwet gelden, met inachtneming van de eisen die artikel 8 EVRM stelt. Voor zover verkeersgegevens de inhoud van communicatie betreffen, zullen deze wel onder de reikwijdte van artikel 13 Grondwet komen te vallen. Aandacht verdient in dit verband dat de inhoud van telecommunicatie in technische zin soms als een verkeersgegeven wordt gezien. Zo wordt het onderwerp van een e-mail in technische zin 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 een sms-bericht omvat tevens de inhoud van communicatie. In veel adviezen over het onderhavige voorstel is nadere aandacht gevraagd voor de afbakening tussen verkeersgegevens en inhoud, omdat door de technologische ontwikkelingen een strikte scheiding tussen inhoud- en verkeersgegevens problematisch zou zijn. In verband met die afbakening hebben wij ten behoeve van dit wetsvoorstel, zoals eerder opgemerkt, onderzoek laten verrichten naar de juridische en technische kwalificatie van verkeersgegevens.[43] De centrale onderzoeksvraag was: Welke typen verkeersgegevens moeten juridisch beschermenswaardig worden geacht onder artikel 13, gelet op de ratio en functie van het communicatiegeheim, en in hoeverre zijn deze typen juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit? Smits omschrijft verkeersgegevens als gegevens die worden verwerkt voor het overbrengen van

[40] 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. Zo ook *Digital Rights* t. *Ierland en Kärntener Landesregierung* t. *Seitlinger*, HvJ EU, C-293/12 en C-594/12 van 8 april 2014 par. 28.

[41] Rapport staatscommissie Grondwet 2010, p. 89. Het lid Overkleeft-Verburg wenste verkeersgegevens wel onder de reikwijdte van artikel 13 te brengen, zie p. 88 van het rapport.

[42] Kamerstukken II 1996/97, 25 433, nr. 3, blz. 3–4.

[43] J.M. Smits, Technische kwalificatie van verkeersgegevens ten behoeve van de herziening van artikel 13 Nederlandse Grondwet, februari 2013; B.J. Koops, Juridische kwalificatie van verkeersgegevens in het licht van artikel 13 Grondwet, februari 2013.

communicatie of voor de facturering van de dienst. Koops omschrijft verkeersgegevens als gegevens die onder de verantwoordelijkheid van de transporteur (als transporteur) vallen, terwijl de inhoud van communicatie volgens hem datgene is wat onder de verantwoordelijkheid van de verzender of ontvanger valt (en niet van de transporteur). De onderzoekers menen dat het onderscheid tussen inhoud en verkeersgegevens met name waar het communicatie via internettoepassingen betreft soms lastig is te maken, met uitzondering van e-mail. Het onderzoek van Smits toont aan dat er grijze gebieden bestaan tussen de inhoud van communicatie en verkeersgegevens bij het gebruik van bepaalde applicaties en internetprotocollen. Voorbeelden hiervan zijn surfgegevens, en het gebruik van bepaalde informatienummers of poortnummers waaruit de strekking van communicatie kan worden afgeleid, maar niet de (letterlijke) inhoud van die communicatie. Categorieën van verkeersgegevens (in technische zin) kunnen niettemin nader worden geclassificeerd naar gelang de manier waarop of de mate waarin zij samenhangen met de inhoud van communicatie. Dat gegevens die de inhoud van de communicatie betreffen in technologische optiek als verkeersgegevens worden beschouwd, doet niet af aan de bescherming van artikel 13. Zo betreffen het sms-bericht en de onderwerpregel van een e-mail de inhoud van communicatie, omdat deze onder de verantwoordelijkheid van de verzender vallen. Zij geven de gevoelens of gedachten weer die de verzender wenst over te brengen naar een of meer ontvangers zonder dat anderen daarvan kennis kunnen nemen. De bestaande wetgeving merkt de hier genoemde voorbeelden van de onderwerpregel van een e-mail en een sms overigens evenmin aan als verkeersgegevens. Verkeersgegevens die geen betrekking hebben op de inhoud van communicatie vallen echter buiten de reikwijdte van artikel 13. De wetgever en de rechter zullen bij de verdere ontwikkeling van communicatietechnieken en indien nodig in het concrete geval steeds moeten bepalen wanneer bepaalde verkeersgegevens de inhoud van communicatie betreffen, en dientengevolge de bescherming van artikel 13 genieten.

2.4. Toepassing van het communicatiegeheim in horizontale verhoudingen

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.[44] 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.[45] Dit is reeds erkend door de grondwetgever van 1983.
Bestaande wetgeving geeft reeds een nadere uitwerking van het brief- en telecommunicatiegeheim in horizontale verhoudingen. De wetgever verplicht postvervoerbedrijven die vallen onder de toepassing van de Postwet 2009, in artikel 4 van de Postwet 2009 om het grondwettelijke briefgeheim te eerbiedigen. Bovendien kent de Telecommunicatiewet een uitgewerkte borging van het telecommunicatiegeheim. De verplichting in de Telecommunicatiewet om de vertrouwelijkheid van communicatie te respecteren is gericht tot aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten. Aanbieders van diensten van de informatiemaatschappij die

---

[44] L.F.M. Verhey, *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy* (diss. Utrecht) 1992.

[45] 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).

betrokken zijn bij communicatie via openbare elektronische communicatienetwerken zoals Gmail en Twitter vallen hier thans niet onder. De Telecommunicatiewet richt zich bovendien exclusief op normadressaten met een openbaar karakter. Elektronische netwerken en elektronische diensten met een besloten karakter, zoals interne e-maildiensten en toegang tot het intranet van een werkgever, vallen buiten het bereik van de Telecommunicatiewet. Het communicatieverkeer dat plaatsvindt in netwerken en diensten met een besloten karakter is daarmee niet geheel onttrokken an wettelijke bescherming voor wat betreft het communicatiegeheim. Zo geldt voor aanbieders van diensten van de informatiemaatschappij de Wet bescherming persoonsgegevens (Wbp). In besloten netwerken bieden de beginselbepalingen in het Burgerlijk Wetboek (het «goed werkgeverschap» ex artikel 7:611 BW kan indien nodig door de rechter voor wat betreft het belang bij het brief- en telecommunicatiegeheim nader worden ingevuld) en de Wbp bescherming. De werksfeer is bijvoorbeeld geen privésfeer, al mogen werknemers binnen grenzen wel een redelijke verwachting van privacy koesteren in hun werkomgeving. Het adequaat informeren van de werknemer door de werkgever vervult in dat kader een belangrijke rol bij de beoordeling van de beperking van het brief- en telecommunicatiegeheim van de werknemer. In voorkomende gevallen past een belangenafweging door de rechter. De Wbp en andere wettelijke bepalingen bieden hiervoor voldoende houvast. De Wbp is ook van toepassing op de verwerking van persoonsgegevens door aanbieders van sociale media en webmail.
De reikwijdte van artikel 13 strekt tot bescherming van de burger tegen inbreuken op het communicatiegeheim door de overheid. 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 brief- en telecommunicatiegeheim in private verhoudingen. Zowel het rapport van de Commissie-Franken als het wetsvoorstel van het toenmalige kabinet bevatten destijds een voorziening 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 op haar beurt geen beschouwing aan een dergelijke regelingsopdracht en heeft hiervoor dan ook geen voorstel gedaan. Volgens het toenmalige kabinet was een verdergaande regeling van de horizontale werking dan een regelingsopdracht aan de gewone wetgever binnen het kader van hoofdstuk 1 van de Grondwet niet goed denkbaar.
Wij hebben overwogen, gelet op de ontwikkelingen in de communicatietechnologie, de opkomst van private partijen en de betekenis van communicatie in de samenleving, een derde lid met een regelingsopdracht voor de wetgever op te nemen. Daar is van afgezien omdat een dergelijke regelingsopdracht niet noodzakelijk is, gelet op de bepalingen die reeds zijn opgenomen in de Postwet en de Telecommunicatiewet (mede op basis van de Privacyrichtlijn) om de toepassing van het communicatiegeheim in horizontale verhoudingen te borgen.[46] De omstandigheid dat bij internetverkeer gegevens ook buiten Nederlands grondgebied kunnen worden getransporteerd doet er niet aan af dat een ieder die binnen de Nederlandse rechtsmacht opereert, het communicatiegeheim dient te respecteren. Dit uitgangspunt is voor horizontale

[46] De toezegging van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de suggesties van het lid Swagerman (VVD) ten aanzien van horizontale werking te betrekken bij het Wetsvoorstel tot wijziging van artikel 13 Grondwet, zijn hiermee gestand gedaan (Handelingen I 2011–2012, nr. 18–3 – blz. 28).

verhoudingen vastgelegd in artikel 11.2.a Telecommunicatiewet (Tw). Ook dient de overheid op grond van de jurisprudentie inzake artikel 8 EVRM in adequate oplossingen te voorzien wanneer het communicatiegeheim in horizontale relaties aan de orde is. Zonder grondwettelijke regelingsopdracht is het communicatiegeheim in horizontale relaties voldoende geborgd. Tot slot dient te worden voorkomen dat rechtsonzekerheid ontstaat over de reikwijdte van artikel 13. Communicatiestromen en de opslag van gegevens onttrekken zich voor een deel aan de controle van de gebruikers en de Nederlandse overheid vanwege het feit dat de gegevensstromen zich ook buiten het Nederlandse grondgebied verplaatsen. Voor bescherming in die gevallen zijn gebruikers in het buitenland afhankelijk van de wetgeving en controle op de naleving daarvan door staten waar de communicatie doorheen reist.
De essentie van artikel 13 Grondwet, te weten bescherming tegen heimelijke kennisneming door de overheid van de inhoud van communicatie, om het even met welk middel, blijft zonder het nu geschrapte derde lid onverminderd behouden.

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 de bescherming van de nationale veiligheid. Strafrechtelijke opsporingsautoriteiten en de inlichtingen- en veiligheidsdiensten kunnen kennisnemen van (de inhoud van) communicatie met een machtiging van de rechter respectievelijk door of met machtiging van hen die daartoe bij de wet zijn aangewezen. 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. Dit onderscheid in beschermingsniveau als gevolg van technologische ontwikkelingen achten wij niet langer houdbaar, noch wenselijk. 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. Wij zien 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.[47] 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

[47] Rapport Commissie-Franken, p. 150, 156 en Kamerstukken II 2000/01, 27 460, nr. 1, blz. 27–28.

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 brief- en telecommunicatiegeheim, dus ongeacht de voor de communicatie gebruikte techniek.[48] 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 een rechterlijke machtiging vereist. 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 door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Deze keuzes worden nader toegelicht in respectievelijk 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.[49] 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

---

[48] 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.

[49] Eindrapport «Gegevensvergaring in strafvordering» van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, mei 2001.

moeten worden overgelaten.[50] Wij menen echter dat voor een inbreuk op het brief- en telecommunicatiegeheim een extra grondwettelijke 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.[51] Het stellen van de eis van een rechterlijke machtiging in de Grondwet voldoet aan dat criterium van het EHRM en 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.[52] Zowel de Raad van State als diverse Kamerfracties drongen daar destijds nadrukkelijk op aan bij het toenmalige kabinet.
Wat betreft de verhouding tot andere grondwettelijke grondrechten 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 (artikel 10), te weten de privé-communicatie. 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.[53] 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.

Notificatie

Tot slot heeft de staatscommissie Grondwet heeft in haar rapport uit 2010 zonder nadere toelichting afgezien van een notificatieplicht. Wij zien evenmin noodzaak tot het op constitutioneel niveau verankeren van een notificatieplicht zoals door een aantal organisaties is geadviseerd. Zoals zij betogen kan een notificatieplicht de toegang tot rechtsbescherming van de burger verhogen, maar dit is nog geen argument om de notificatieplicht ook in de Grondwet op te nemen, mede gelet op het sobere karakter van de huidige Grondwet. Wij zijn van mening dat of en wanneer notificatie aangewezen is een afweging is die door de wetgever moet worden gemaakt. Daarbij kunnen de administratieve lasten die voortvloeien uit de opname van een notificatieplicht in wetgeving per categorie

---

[50] 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 toenmalige kabinet echter is teruggekomen bij nota van wijziging (Kamerstukken II 1997/98, 25 443, nr. 6).

[51] *Valentino Acatrinei* t. *Roemenië*, EHRM 25 juni 2013, nr. 18540/04, par. 58; *Iordachi e.a.* t. *Moldavië*, EHRM 14 september 2009, nr. 25198/02, par. 40 en *Dumitru Popescu* t. *Roemenië*, EHRM 26 april 2007, nr. 71525/01, par. 70–73, *Klass* t. *Duitsland*, EHRM 6 september 1978, series A 28, par. 55–56.

[52] 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).

[53] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 41.

gevallen worden afgewogen tegen de beoogde rechtswaarborg. Het kan in voorkomende gevallen bovendien noodzakelijk zijn, de balans tussen enerzijds de mate van noodzakelijke heimelijkheid voorafgaand aan observatie of inzage en anderzijds een effectieve bescherming van het recht op het brief- en communicatiegeheim, achteraf te herstellen met een notificatieplicht.[54]

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.[55] Een toets door de rechter voorafgaand aan het onderscheppen van bij een derde in beheer zijnde communicatie van burgers, denk aan het openen van (elektronische) post, en het tappen van telefoongesprekken of communicatie die verloopt via internet, heeft een zelfregulerend effect op de uitvoeringspraktijk. Het werpt een natuurlijke drempel op, die naar ons oordeel nodig is om willekeurig gebruik van deze zwaar op de persoonlijke levenssfeer ingrijpende bevoegdheden te voorkomen. Wij zijn van mening dat deze toets vanuit een oogpunt van *checks and balances* het best kan worden uitgevoerd door een rechter, die vanuit een ander perspectief naar grondrechtelijke beperkingen kijkt dan de uitvoerende macht.[56] 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. Hoewel in diverse adviezen is betoogd dat ook beperkingen in het belang van de nationale veiligheid, gelet op dergelijke checks and balances, bij voorkeur door een rechter zouden moeten worden getoetst, valt de belangenafweging daar wat ons betreft anders uit (zie par. 3.3). Wel zal sprake moeten zijn van enige andere vorm van onafhankelijke toezicht, waarin is voorzien door de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002).
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 (artikel 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.
In reactie op diverse adviezen merken wij op dat het toetsingskader van de rechter om te beoordelen of hij al dan niet een machtiging afgeeft die een inbreuk op het brief- en telecommunicatiegeheim toestaat, grotendeels is ontleend aan de eisen die voortvloeien uit het EVRM, te weten noodzakelijkheid, subsidiariteit en proportionaliteit. De nationale rechter beoordeelt telkens of er voor een inbreuk op het brief- en telecommunicatiegeheim een dwingende maatschappelijke noodzaak is, of de inzet van de betreffende bijzondere opsporingsbevoegdheid een geschikt middel

---

[54] De Minister van Binnenlandse Zaken en Koninkrijksrelaties doet hiermee gestand aan zijn toezegging, de suggesties van het lid Swagerman (VVD) ten aanzien van het al of niet invoeren van een notificatieplicht te betrekken bij dit wetsvoorstel (Handelingen I 2011/12, nr. 18–3 – blz. 28).

[55] 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.

[56] Vgl. *Iordachi e.a.* t. *Moldavië,* EHRM 14 september 2009, nr. 25198/02, par. 40 en *Dumitru Popescu* t. *Roemenië,* EHRM 26 april 2007, nr. 71525/01, par. 70–73.

vormt om het beoogde doel te bereiken en in een redelijke en evenredige verhouding staan tot dat beoogde doel. Deze eisen vloeien voort uit het EVRM en zijn daarnaast ten dele gecodificeerd in nationale wetgeving. De betreffende strafvorderlijke bepalingen, bijvoorbeeld artikel 126m Sv inzake het opnemen van communicatie, stellen als wettelijke eis dat de inzet van de opsporingsbevoegdheid alleen is toegestaan indien het onderzoek dit dringend vordert. Voorts moet het gaan om een verdenking van misdrijven van een zekere ernst, bijvoorbeeld in het geval van artikel 126m Sv om een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.

3.3. Beperkingen in het belang van de nationale veiligheid

Uitzondering op de hoofdregel dat voor beperkingen van het brief- en telecommunicatiegeheim een rechterlijke machtiging nodig is, is dat op grond van het tweede lid in het belang van de nationale veiligheid beperkingen zijn toegestaan door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Deze formulering sluit aan bij de formulering van het huidige artikel 13, tweede lid, voor de middelen telefoon en telegraaf. In de consultatieversie van het wetsvoorstel was gekozen voor de formulering «met machtiging van een of meer Ministers». De toelichting daarop riep blijkens de adviezen onduidelijkheid op ten aanzien van de mogelijkheden om de bevoegdheid tot het verlenen van een machtiging te mandateren. Bovenal kiezen wij thans voor de formulering «door of met machtiging van hen die daartoe bij de wet zijn aangewezen», omdat het onder de oorspronkelijk voorgestelde formulering niet mogelijk zou zijn om in bepaalde bijzondere gevallen op wettelijk niveau ook voor beperkingen op het brief- en telecommunicatiegeheim in het belang van de nationale veiligheid te eisen dat de rechter de machtiging geeft, terwijl die optie wel gewenst is. Te denken valt aan de situatie waarin sprake is van het achterhalen van bronnen van journalisten met het oog op de persvrijheid. Naar aanleiding van de uitspraak van het EHRM in de Telegraafzaak[57], waaraan ook in de adviezen van het CRM, NJCM en Privacy First is gerefereerd, heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties een wijziging van de Wiv 2002 aangekondigd, waarin zal worden bepaald dat er een onafhankelijke bindende toets door de rechter wordt verricht voorafgaand aan de inzet van bijzondere bevoegdheden, waaronder de gerichte interceptie van communicatie, jegens journalisten, welke gericht is op het achterhalen van hun bronnen. Anders dan in diverse adviezen naar voren is gebracht zien wij geen noodzaak tot het eisen van een rechterlijke machtiging voor alle beperkingen in het belang van de nationale veiligheid op het niveau van de Grondwet. Dat eist de jurisprudentie van het EHRM, anders dan betoogd, naar onze mening niet. Het EHRM stelt in de zaak *Klass t. Duitsland* dat, hoewel rechterlijke controle in beginsel wenselijk zou zijn, het in casu fungerende Duitse systeem van toezicht door de parlementaire toezichtcommissie en de zogenoemde G10-commissie in overeenstemming is met artikel 8 EVRM. Die twee organisaties zijn voldoende onafhankelijke autoriteiten met afdoende bevoegdheden voor een effectieve controle op het functioneren van de inlichtingendiensten: «Nevertheless, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the Court concludes that the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society.»[58] Meer recente jurisprudentie

[57] EHRM 22 november 2012, Telegraaf Media Nederland Landelijke Media BV e.a. t. Nederland, nr. 39315/06.
[58] *Klass* t. *Duitsland*, EHRM 6 september 1978, series A 28, par. 56.

leidt niet tot een andere conclusie.[59] De nu voorgestelde formulering van artikel 13, tweede lid, geeft ruimte voor maatwerk op het niveau van de wetgever en is in overeenstemming met de jurisprudentie van het EHRM. Wat betreft de functionarissen die bij wet kunnen worden aangewezen om het grondrecht te beperken, valt op te merken dat dit in aansluiting op de Wiv 2002 in de hoofdregel één of meer Ministers zullen zijn. In bijzondere gevallen, zoals hierboven geschetst, kan de rechter worden aangewezen. Hiermee wordt aangesloten bij de huidige systematiek van de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten in de Wiv 2002 (zie paragraaf 6.3 hierna) voor andere communicatiemiddelen dan de brief, waarvoor 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.[60] Deze argumentatie is 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. De taakopdracht van de inlichtingen- en veiligheidsdiensten, AIVD en MIVD, is naar zijn aard noodzakelijkerwijs relatief open geformuleerd en zal – mede afhankelijk van de gepercipieerde dreiging van de nationale veiligheid – invulling krijgen. Deze invulling dient onder verantwoordelijkheid van de voor de diensten verantwoordelijke Ministers – en waar het gaat om het onderzoek naar andere landen, mede onder de verantwoordelijkheid van de Minister van Algemene Zaken en van Buitenlandse Zaken – plaats te vinden. Er is evenwel geen sprake van een ongeclausuleerde of ongecontroleerde bevoegdheidsuitoefening. De Wiv 2002 bevat een duidelijk kader met controlemechanismen. De inlichtingen- en veiligheidsdiensten mogen bijzondere bevoegdheden alleen dan toepassen indien dat noodzakelijk is voor de goede uitvoering van de aan de diensten opgedragen taken en met inachtneming van de eisen van proportionaliteit en subsidiariteit, welke criteria zijn ontleend aan de jurisprudentie van het EHRM (zie par. 6.3). Het geheel aan bevoegdheden die een inlichtingen- en veiligheidsdienst ter beschikking staan om onderzoek te doen, vergt een voortdurende afweging. De Minister is in dezen beter geïnformeerd dan de rechter en kan tot een integrale afweging komen over de inzet daarvan. Over de wijze waarop aan die taak invulling wordt gegeven dient de voor de desbetreffende dienst verantwoordelijke Minister in het jaarlijks voor 1 mei uit te brengen jaarverslag over de taakuitvoering van de onder hem ressorterende dienst nadrukkelijk in te gaan op de aandachtsgebieden van het afgelopen en lopende jaar (artikel 8 Wiv 2002). Op deze wijze kan de Minister ter zake van de invulling van de taak van de dienst in het parlement ter verantwoording worden geroepen.
Een niet onbelangrijk aspect bij de keuze om de machtiging in het geval van inlichtingen- en veiligheidsdiensten in de hoofdregel bij de Minister te laten, vormt de internationale component van de taakuitvoering van de diensten, zoals het verrichten van onderzoek *naar* andere landen en het verrichten van zelfstandig, heimelijk onderzoek *in* die landen, hetgeen de toepassing van bijzondere inlichtingenmiddelen met zich brengt. Dat is bij uitstek een aangelegenheid die tot de competentie en de verantwoordelijkheid van de voor de diensten verantwoordelijke Ministers behoort. Beide aspecten brengen immers politieke risico's met zich mee, zoals schade aan de betrekkingen tussen Nederland en andere landen, kans op diplomatieke tegenmaatregelen en – bij onderkenning – mogelijk ook gevolgen voor de veiligheid van de personen die door de dienst in dit kader in het buitenland zijn ingezet. Bovendien gaat het bij onderzoek naar

[59] Bijv. *Kennedy* t. *het Verenigd Koninkrijk*, EHRM 18 mei 2010, nr. 26839/05, par. 155–170.
[60] Kamerstukken II 1997/98, 25 443, nr. 5, blz. 12–13.

andere landen in het kader van de buitenlandtaak van de diensten om het vergaren van (politieke) inlichtingen die in het bijzonder voor het te voeren buitenlands beleid van Nederland van belang zijn. De wettelijke regeling waarin de taak en bevoegdheden van de inlichtingen- en veiligheidsdiensten is geregeld, waaronder de bevoegdheid tot het ontvangen en opnemen van telecommunicatie en het openen van brieven en andere geadresseerde zendingen, kent geen extraterritoriale werking. Niettemin wordt – zoals indertijd bij de parlementaire behandeling van de Wiv 2002 is aangegeven – de Wiv 2002 ter zake *naar analogie* toegepast. Op deze manier wordt zeker gesteld dat ook in die situaties een toets plaatsvindt aan de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit en dat daaromtrent verantwoording kan worden afgelegd alsmede effectief toezicht door de CTIVD mogelijk is. Het leggen van de bevoegdheid tot het verlenen van machtiging bij de toepassing van bijzondere inlichtingenmiddelen in andere landen, in casu de interceptie van telecommunicatie, bij een rechterlijke instantie zal gelet op het ontbreken van jurisdictie er in de praktijk toe leiden dat verzoeken daartoe door de Nederlandse rechter niet zullen (kunnen) worden gehonoreerd. Dat vormt een onaanvaardbaar risico voor de nationale veiligheid.
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. Bij alle door de inlichtingen- en veiligheidsdiensten uit te oefenen bijzondere bevoegdheden is in meer of mindere mate sprake van een beperking van het recht op bescherming van de persoonlijke levenssfeer. Het beleggen van de bevoegdheid tot het verlenen van een machtiging met betrekking tot een enkele bijzondere bevoegdheid bij een andere instantie, te weten de rechter, dan waarvoor binnen het stelsel van de Wiv 2002 door de wetgever is gekozen, te weten de Minister, komt tegen deze achtergrond bezien dan ook arbitrair over.
Delegatie van de machtigingsbevoegdheid is in het voorgestelde artikel 13, tweede lid, evenals in de huidige (oude) bepaling, uitgesloten. Gelet op de formulering van het tweede lid is het aan de wetgever om te bepalen aan wie de bevoegdheid tot het maken van een inbreuk op het grondwettelijke brief- en telecommunicatiegeheim dient toe te komen en aldus ook in welke gevallen er ruimte wordt geboden om het geven van een machtiging in mandaat uit te oefenen. In reactie op de adviezen van de CTIVD en het CRM, die op basis van de toelichting vragen hadden bij de ogenschijnlijk algemene mogelijkheid tot mandaat, merken wij op dat in ieder geval niet is beoogd ruimere mogelijkheden tot mandaat toe te staan dan onder het huidige artikel 13. Voor zover er mandaat is verleend, wordt deze 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 onvermijdelijke inbreuken door 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».[61] Artikel 13 EVRM, dat 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 onafhankelijk toezicht op de diensten noodzakelijk is.[62] Van belang hierbij

[61] *Segerstedt-Wiberg e.a.* t. *Zweden,* EHRM 6 juni 2006, par. 117.
[62] *Kennedy* t. *Verenigd Koninkrijk,* EHRM 18 mei 2010, par. 167.

is dat het geheel aan toezichts- en controlemechanismen in ogenschouw genomen moet worden. Het toezicht op de inlichtingen- en veiligheidsdiensten is in het bijzonder belegd bij de CTIVD. Zoals de Minister van Binnenlandse Zaken in het Algemeen overleg naar aanleiding van de evaluatie van de Wiv 2002 heeft toegezegd zal de CTIVD als onafhankelijke klachtinstantie worden gepositioneerd met de bevoegdheid om bindende oordelen te geven op klachten.[63]
Voorts is sprake van parlementaire controle. Er wordt zowel in het openbaar als vertrouwelijk waar het gaat om operationele activiteiten van de diensten, te weten in de Commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer, door de betreffende Ministers omtrent de taakuitvoering door de AIVD en de MIVD verantwoording afgelegd. Daarnaast bestaat de mogelijkheid tot indienen van een klacht bij de Nationale ombudsman en ook de rechter kan in daartoe in aanmerking komende gevallen worden geadieerd. 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.
Het voorgestelde grondwettelijke systeem heeft tot gevolg dat anders dan onder het huidige artikel 13, eerste lid, het briefgeheim in het belang van de nationale veiligheid voortaan zonder rechterlijke machtiging zou kunnen worden beperkt, *als* artikel 23 van de Wiv 2002 daartoe zou worden aangepast. Die bepaling wijst thans de rechtbank Den Haag exclusief aan als bevoegd tot het afgeven van een last. Ook voor het openen van brieven in het belang van de nationale veiligheid zal gaan gelden dat dit grondwettelijk is toegestaan door of met machtiging van hen die daartoe bij de wet zijn aangewezen. 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 in par. 2.1.2 zijn genoemd. Zoals is opgemerkt in paragraaf 3.1 willen wij 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. Het CRM is van mening dat de uniformiteit van het regime onvoldoende reden is om het beschermingsniveau van de brief te verlagen. In dat opzicht wijzen wij erop dat de wetgever kan bepalen om de eis van een rechterlijke last voor een brief in de Wiv 2002 te handhaven.
Waar inbreuken op het brief- en telecommunicatiegeheim in het belang van de nationale veiligheid kunnen plaatsvinden zonder voorafgaande controle door een onafhankelijke instantie is zoals gezegd een adequate alternatieve vorm van toezicht nodig op de toepassing van deze bevoegdheid door de inlichtingen- en veiligheidsdiensten. 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.[64] In dat verband stelde de Raad dat overwogen zal moeten worden dat toezicht grondwettelijk te verankeren (p. 9). Het CRM adviseerde een onafhankelijke vorm van toezicht, door een functionaris buiten de organisatie, op de inlichtingen- en veiligheidsdiensten in de Grondwet te verankeren. 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

[63] Toegezegd door de Minister van Binnenlandse zaken en Koninkrijksrelaties tijdens een Algemeen overleg over het evaluatierapport van de Commissie Dessens (16 april 2014).
[64] *Klass* t. *Duitsland*, EHRM 6 september 1978, series A 28, par. 55–56.

de artikelen 64 en volgende van de wet).[65] 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 of dergelijk onafhankelijk toezicht in de praktijk bestaat en effectief is. Internationaal recht vereist aldus niet dat grondwettelijk wordt voorgeschreven dat bij het ontbreken van rechterlijk toezicht ten aanzien van de beperking van een specifiek grondrecht wordt voorzien in een andere vorm van onafhankelijk toezicht. Zowel in de bijdragen ontvangen tijdens de internetconsultatie als in diverse adviezen is aandacht gevraagd voor voldoende checks en balances met betrekking tot het toezicht op bevoegdheidsuitoefening door de inlichtingen- en veiligheidsdiensten. Geadviseerd is onder andere om te onderzoeken of een krachtiger toezichtorgaan naar Duits of Belgisch model kan worden opgericht. Wij merken op dat sturing en toezicht op de taakuitoefening door de inlichtingen- en veiligheidsdiensten een specifiek aandachtspunt is geweest in de evaluatie van de Wiv 2002.[66] Het ligt meer voor de hand eventuele wijzigingen in het algehele toezichtsysteem – die bovendien algemener van aard kunnen zijn dan in verband met het onderhavige voorstel – te bespreken in het kader van het evaluatierapport van deze commissie en de daarop volgende discussie over een eventuele wijziging van de Wiv 2002. In dat verband dient hier te worden opgemerkt dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties bij de gelegenheid van een algemeen overleg heeft toegezegd dat de CTIVD als zelfstandige klachtinstantie de bevoegdheid krijgt tot het geven van bindende oordelen.[67] Daarnaast zal in de wet worden voorzien in een verplichte heroverweging door de Minister, indien de CTIVD van oordeel is dat een verleende toestemming van de Minister voor de inzet van bijzondere bevoegdheden niet in overeenstemming is met de wet. Indien de Minister geen reden ziet om de verleende toestemming in te trekken, dan dienen de CTIVD en de CIVD onverwijld over dat besluit te worden geïnformeerd. De CIVD kan dan de betreffende Minister ter verantwoording roepen.[68]De Wiv 2002 zal in die zin worden aangepast. Het voorgestelde artikel 13 van de Grondwet laat de wetgever de ruimte om het onafhankelijke toezicht zo in te vullen als hij op basis van de uitkomsten van de evaluatiecommissie noodzakelijk acht.

«Nationale veiligheid»

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. Ook in enkele adviezen over het onderhavige voorstel is opgemerkt dat het begrip nationale veiligheid lastig af te bakenen is. 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 over artikel 8 EVRM, 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

---

[65] Kamerstukken II 1997/98, 25 877, nr. 3, blz. 77.
[66] Zie Kamerstukken II 2011/12, 29 924, nr. 91.
[67] AO 16 april 2014, conceptverslag blz. 32–33.
[68] Kamerstukken II 2013/14, 33 820, nr. 2, blz. 6.

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. Ook op het terrein van de cybersecurity kan sprake zijn van de vervulling van taken door overheidsdiensten in het belang van de nationale veiligheid. 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). Dit doelcriterium van de nationale veiligheid begrenst dus ook de bevoegdheden van de inlichtingen- en veiligheidsdiensten. 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 AIVD en de MIVD op grond van de Wiv 2002. Bij de totstandkoming van die bepalingen is reeds uitvoerig op de betekenis van het begrip ingegaan.[69] Er is geen sprake van dat het begrip nationale veiligheid in het kader van de bevoegdheden tot het intercepteren van communicatie wordt opgerekt. Het CRM plaatst, net als de Raad van State in 2002, 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 en stelt dat het daarom slechts een geschikt criterium is in combinatie met de overige randvoorwaarden die het EVRM daaraan stelt: 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. Hoewel zonder meer duidelijk is wat de rechtsstatelijke waarde is van een noodzakelijkheids- en proportionaliteitstoets en deze ook door de bevoegde instanties zal moeten worden verricht bij het al dan niet afgeven van een machtiging, stellen wij niet voor om die toetsingscriteria expliciet in het onderhavige voorstel op te nemen. Wij kiezen met dit voorstel bewust voor een beperkte modernisering van de Grondwet: een uitbreiding van de reikwijdte van artikel 13 naar alle communicatiemiddelen. 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 Grondwet wel voor ogen had door de combinatie met de door haar voorgestelde algemene aanvullende beperkingsclausule.[70] Wij hechten eraan om nogmaals te benadrukken dat ook onder de Wiv 2002 moet worden getoetst of de inzet van een bijzondere bevoegdheid door de inlichtingen- en veiligheidsdiensten noodzakelijk is en voldoet aan de eisen van subsidiariteit en proportionaliteit. Het doelcriterium van de nationale veiligheid is dus in dat opzicht voorzien van dezelfde randvoorwaarden in de Wiv 2002 als in artikel 8 EVRM. Aan de rechtsbescherming van de burger doet dat intussen al helemaal niet af: indien de wetgever op het brief- en telecommunicatiegeheim een beperking wenst aan te brengen, dient deze onverkort te worden getoetst aan artikel 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 – in het belang van de nationale veiligheid – door of met machtiging van hen die bij de wet daartoe zijn aangewezen – en artikel 8 EVRM stelt de

---

[69] 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.

[70] Zie paragraaf 6.5 en p. 88 van het rapport van de staatscommissie Grondwet.

materiële beperkingsvereisten van noodzakelijkheid en proportionaliteit met het oog op specifiek omschreven doelcriteria.

4. Verhouding tot internationale regelgeving

4.1. Inleiding

In de Nederlandse rechtsorde zijn verschillende internationale verdragen van toepassing 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 dit hoofdstuk gaan wij daarom nader in op het brief- en telecommunicatiegeheim in internationale context.

4.2. EU-recht

4.2.1. 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. Dit blijkt ook uit artikel 52, derde lid, van het Handvest, waarin is bepaald dat voor zover de in het handvest neergelegde rechten corresponderen met de rechten die zijn gegarandeerd in het EVRM, de inhoud en reikwijdte ervan dezelfde zijn als die welk er door het EVRM aan worden toegekend. Om rekening te houden met de technische ontwikkelingen is het woord «correspondentie» in het EU-Handvest vervangen door «communicatie».[71] Gelet op artikel 52, derde lid, van het Handvest, zal het Hof van Justitie van de EU aan het begrip «communicatie» invulling geven in overeenstemming met de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) ten aanzien van artikel 8 EVRM.[72] Van belang is hierbij aan te tekenen dat het Handvest en derhalve ook artikel 7 EU-Handvest, voor de lidstaten uitsluitend van toepassing is wanneer de lidstaten het recht van de Unie ten uitvoer leggen (artikel 51, eerste lid, EU-Handvest). Het Handvest heeft dus geen zelfstandige betekenis in situaties waarin Nederland niet het recht van de Unie ten uitvoer legt.

[71] 2007/C303/02.
[72] Zie voor de interpretatie van het EU-Handvest in het licht van het EVRM de artikelen 51–54 van het EU-Handvest, en specifiek artikel 52 lid 3.

4.2.2. Secundair EU-recht

In het secundaire EU-recht zijn in verband met het brief- en telecommunicatiegeheim vooral de algemene privacyrichtlijn (hierna: Privacyrichtlijn)[73] en de aanvullende sectorale richtlijn voor de sector elektronische communicatie (hierna: ePrivacyrichtlijn)[74] van belang.

De Privacyrichtlijn, welke is geïmplementeerd in de Wbp, ziet op de wijze waarop persoonsgegevens moeten worden beschermd en is ten aanzien van twee aspecten relevant. Allereerst ziet het op de wijze waarop persoonsgegevens, tot personen herleidbare gegevens, dienen te worden beschermd. Daarnaast is de Privacyrichtlijn van betekenis voor de bescherming van verkeersgegevens, welke voor zover ze tot een persoon herleidbaar zijn, immers persoonsgegevens zijn.

Voor verkeersgegevens die worden gegenereerd bij elektronische communicatie was de zogenoemde Dataretentierichtlijn uit 2006 van belang voor de nationale wetgeving met betrekking tot de bewaring van verkeersgegevens ten behoeve van de opsporing en vervolging van strafbare feiten.[75] De Dataretentierichtlijn, die een aanvulling op de eerdergenoemde ePrivacyrichtlijn vormde, beoogde de wetgeving van de EU-lidstaten te harmoniseren, waarbij aan de aanbieders van elektronische communicatiediensten of -netwerken een verplichting tot bewaring van bepaalde aangewezen verkeersgegevens diende te worden opgelegd ten behoeve van de opsporing en vervolging van ernstige strafbare feiten, voor een periode van ten minste zes en ten hoogste vierentwintig maanden. De Dataretentierichtlijn is in Nederland geïmplementeerd in de Wet bewaarplicht telecomgegevens (zie hierna par. 5.5). Het Hof van Justitie van de EU verklaarde echter op 8 april 2014 de Dataretentierichtlijn in *Digital Rights t. Ierland en Kärntner Landesregierung t. Seitlinger* strijdig met de artikelen 7, 8 en 11 van het EU-Handvest en verklaarde de gehele richtlijn ongeldig.[76] In deze uitspraak is met name de persoonlijke levenssfeer van burgers aan de orde in het licht van het grootschalig verzamelen van gegevens die nauwkeurige aanwijzingen kunnen bevatten over het privéleven van degenen van wie de gegevens worden bewaard. Het Hof stelt voor het maken van inbreuken strikte eisen aan een dergelijke gegevensverzameling en -bewaring; deze hebben zowel betrekking op de noodzaak en proportionaliteit van een dergelijke gegevensopslag als de waarborgen voor een effectieve bescherming tegen het risico van misbruik en onrechtmatige toegang tot de gegevens. Er is nog geen definitieve duiding van de gevolgen van de Hofuitspraak. De Europese Commissie beraadt zich thans over een nieuwe richtlijn voor de bewaring van verkeersgegevens ten behoeve van de opsporing en vervolging van strafbare feiten, binnen de door het Hof geformuleerde kaders.

Naast het algemene kader van de Privacyrichtlijn werd een specifiek op de telecommunicatiesector toegesneden aanvullende regeling noodzakelijk geacht. De ePrivacyrichtlijn, welke is geïmplementeerd in de Telecommunicatiewet (Tw), beschermt de persoonlijke levenssfeer van gebruikers van openbare elektronische communicatienetwerken en -diensten. Hoewel de

---

[73] 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 (PbEU 1995, L 281). Momenteel wordt binnen de EU onderhandeld over de wijziging van de Privacyrichtlijn in een Verordening (COM(2012) 11 final, 2012/0011 (COD).

[74] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, (PbEU 2002, L 201).

[75] 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, (PbEU 2006, L 105). Zie de Wet bewaarplicht telecommunicatiegegevens, Kamerstukken I 2007/08, 31 145, nr. A.

[76] HvJ EU, C-293/12 en C-594/12 van 8 april 2014.

ePrivacyrichtlijn werking in verticale verhoudingen niet uitsluit, beheerst deze vooral horizontale rechtsrelaties: artikel 5, eerste lid, verplicht de lidstaten om het vertrouwelijke karakter van de communicatie en daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische communicatiediensten, voor het overgrote deel private ondermeningen, te garanderen. De ePrivacyrichtlijn is ook van toepassing op de verwerking van verkeersgegevens die geen persoonsgegevens zijn. 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 ePrivacyrichtlijn. 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 Privacyrichtlijn.
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 beschermen.

4.3. Internationale verdragen

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 artikel 8 EVRM en artikel 17 IVBPR. Van deze beide artikelen heeft artikel 8 EVRM de meest vergaande invloed op de bescherming van het huidige brief- telefoon- en telegraafgeheim.
De jurisprudentie van het EHRM heeft aan de betekenis van artikel 8 EVRM een belangwekkende bijdrage geleverd. Het EHRM acht het correspondentiegeheim van groot belang voor de democratie. Artikel 8 EVRM noemt onder meer «respect for his private life» en «correspondence». «Correspondence» kent hetzelfde beschermingsregime als het algemene recht op bescherming van de persoonlijke levenssfeer. 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 van 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.[77] Zowel e-mail als het bezoek van pagina's op het internet vallen onder de reikwijdte van artikel 8 EVRM.[78] Het Hof heeft het recht op respect voor «correspondence» steeds uitgelegd tegen de

---

[77] 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.
[78] *Copland* t. *Verenigd Koninkrijk*, EHRM 3 april 2007, nr. 62617/00.

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 was 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.[79] De specifieke inhoud van communicatie, in dit geval de conversatie over de criminele activiteiten, kan geen aanleiding zijn om deze buiten de reikwijdte van het correspondentiegeheim te houden. 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, ongeacht de inhoud van de communicatie («geen boodschap aan de boodschap»).
Uit de jurisprudentie blijkt dat het Hof voor een benadering kiest waarin ruimte is voor telecommunicatie als onderdeel van «privé-leven» alsook als onderdeel van «correspondentie».[80] 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.[81] 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 door de werkgever plaatsvindt.[82]
Artikel 8 EVRM eist dat beperkingen van het correspondentiegeheim zijn gebaseerd op een voor eenieder toegankelijke en voorzienbare wettelijke regeling en noodzakelijk zijn in een democratische samenleving in het belang van de in het tweede lid genoemde doeleinden, hetgeen inhoudt dat de beperking proportioneel moet zijn in verhouding tot het doel dat ermee wordt gediend. De nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, voorkoming van wanordelijkheden of strafbare feiten, de bescherming van de gezondheid of de goede zeden, of de bescherming van de rechten en vrijheden van anderen vormen een legitiem doel voor beperkingen. Artikel 8 EVRM 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, of in het belang van de nationale veiligheid door of met machtiging van hen die daartoe bij wet zijn aangewezen, 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.[83] Bepalend is immers het beginsel dat de verschillende stelsels

---

[79] *A. t Frankrijk*, EHRM 23 november 1993, series A vol 277-B, par. 34 e.v.
[80] *Copland* t. *Verenigd Koninkrijk*, EHRM 3 april 2007, nr. 62617/00.
[81] *Halford* t. *Verenigd Koninkrijk*, EHRM 25 juni 1997, nr. 20605/92.
[82] *Copland* t. *Verenigd Koninkrijk*, EHRM 3 april 2007, nr. 62617/00.
[83] Opgemerkt zij dat het Hof van Justitie in de zaak Melloni (HvJ, 26 februari 2013, C-399/11, par. 60) heeft bepaald dat nationaal (constitutioneel) recht dat verdergaande bescherming biedt dan het EU-Handvest niet in de weg mag staan aan de voorrang, eenheid en effectieve werking van het Unierecht. Zoals eerder aangegeven in par. 5.1 sluit dit voorstel echter aan bij het beschermingsniveau van het EU-Handvest.

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.

5. Verhouding tot nationale wetgeving

5.1. 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.[84] 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 gedragen, hetgeen zich uit in de vereiste meerderheden in de besluitvormingsprocedures. Zij moeten bovendien zijn ingegeven door een maatschappelijke en juridische noodzaak en het moet gaan om zaken die voldoende constitutionele rijpheid vertonen.[85] 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.[86]
Artikel 13 is een lex specialis van artikel 10. Artikel 10, eerste lid, beschermt het recht op de persoonlijke levenssfeer en vormt de basis voor de volgende leden van artikel 10, alsook voor het bepaalde in de artikelen, 11, 12 en 13. 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. De ratio hiervan is gelegen in het verlies van controle over de inhoud van de communicatie door deze toe te vertrouwen aan een derde en het daarmee samenhangende heimelijke karakter van een inbreuk op de privé-communicatie. 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 als onderdeel van een staatsvrije sfeer van de burger. Het communicatiegeheim en de communicatievrijheid liggen in elkaars verlengde. Het communicatiegeheim staat mede in dienst van het openbaar debat. De vrijheid van meningsuiting wordt immers uitgehold indien het individu niet autonoom kan beslissen over geheim of openbaar communiceren. Er kan, indien de passende waarborgen ontbreken, een verkillend effect op

[84] Vgl. Kamerstukken II 2010/11, nr. 20, blz. 2 en Commissie Franken (2000), p. 46.
[85] Kamerstukken II 2010/11, nr. 20, blz. 4.
[86] Kamerstukken II 2010/11, nr. 20, blz. 10.

de communicatie in de staatsvrije sfeer optreden wanneer die autonomie niet langer gewaarborgd is. De *free market place of ideas* is immers het meest gediend bij de keuzevrijheid van het individu voor geheime of openbare communicatie.[87] 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, gezien het bovenstaande, primair 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.

5.2. Strafrecht

Veel beperkingen op het brief- en telecommunicatiegeheim, alsook de eisen die aan deze beperkingen worden gesteld, zijn vervat in het Wetboek van Strafvordering (Sv). Ook het Wetboek van Strafrecht (Sr) draagt bij aan de bescherming van het brief- en telecommunicatiegeheim, door onder meer computervredebreuk (artikel 138ab Sr) en het aftappen of opnemen van gegevens (artikel 139c Sr) strafbaar te stellen. Voorts is het onttrekken van brieven of andere poststukken aan hun bestemming (artikel 201 Sr), en schending van het brief- en telecommunicatiegeheim door medewerkers van post- en openbare telecommunicatie bedrijven (artikelen 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 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 en 126t Sv kan telecommunicatie die verloopt via de telefoon of het internet worden getapt. Daarnaast bestaat de mogelijkheid om onder nadere voorwaarden van de aanbieder van een communicatiedienst te vorderen dat deze gegevens, niet zijnde 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

[87] Zie ook L.F. Asscher, *Communicatiegrondrechten* (diss. UvA), Amsterdam: Otto Cramwinckel Uitgever 2002, p. 18.

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 (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 gebruikersgegevens. 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 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, een en ander voor zover het daarbij gaat om gegevens die niet voor de aanbieder van de communicatiedienst zijn bestemd of van hem afkomstig zijn.
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.

5.3. 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. Op het wettelijke kader waarbinnen de bevoegdheden van de inlichtingen- en veiligheidsdiensten worden uitgeoefend, is reeds uitvoerig ingegaan in paragraaf 3.3 van de toelichting. Bevoegdheden uit de Wiv 2002 die specifiek kunnen ingrijpen in het brief- en telecommunicatiegeheim zijn het openen van brieven (artikel 23), het binnendringen in een geautomatiseerd werk (artikel 24), het gericht aftappen van elke vorm van gesprek, telecommunicatie of gegevensoverdracht (artikel 25) en het ongericht ontvangen en opnemen alsmede selecteren van niet-kabelgebonden telecommunicatie (artikel 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 (artikel 28). 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 (artikel 18) en met inachtneming van de eisen van proportionaliteit (artikel 31) en subsidiariteit (artikel 32). 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 (artikel 19). De 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 grotendeels al aan bij dit bestaande wettelijke systeem.

5.4. Algemene wet bestuursrecht

In de adviezen is verzocht om aandacht te besteden aan de verhouding van artikel 5:17 Algemene wet bestuursrecht (Awb), welke de bevoegdheid van toezichthouders regelt, tot het onderhavige artikel 13. Op grond van artikel 5:17 Awb is een toezichthouder, iemand die bij of krachtens wettelijk voorschrift met het toezicht op de naleving is belast, bevoegd inzage te vorderen van zakelijke gegevens en bescheiden en daarvan kopieën te maken. De termen «gegevens» en «bescheiden» omvatten ook gegevens die langs elektronische weg zijn vastgelegd. Het gaat in artikel 5:17 Awb om gegevens die gebruikt worden ten dienste van het maatschappelijk verkeer. Gegevens en bescheiden van persoonlijke aard vallen buiten het inzagerecht op grond van artikel 5:17 Awb.[88] Ter ondersteuning van artikel 5:17 Awb regelt artikel 5:20 Awb dat iedereen medewerking moet verlenen bij de uitoefening van die bevoegdheid door de toezichthouder. Op grond hiervan moet een toezichthouder bijvoorbeeld ook toegang tot een computer(bestand) worden verschaft door het verstrekken van wachtwoorden. Toezichthouders kunnen daarin een verzameling correspondentie, die zowel zakelijk als persoonlijk van aard kan zijn, aantreffen. Zoals hiervoor uiteengezet beschermt artikel 13 de inhoud van communicatie, te weten uitwisseling van informatie, gedachten en gevoelens tussen personen of instanties, die is toevertrouwd aan een derde voor transport en/of opslag. Deze bescherming staat niet in de weg aan de hiervoor genoemde medewerkingsplicht. De toezichthouder kan zijn bevoegdheden op grond van titel 5:2 Awb jegens de verzender of ontvanger van communicatie conform de wet uitoefenen. In voorkomend geval kan deze bij hen zakelijke e-mails opvragen of om toegang verzoeken tot de administratie, ook indien deze zich in de cloud bevinden. Daarmee beslaan de bevoegdheden en verplichtingen die voortvloeien uit de artikelen 5:17 en 5:20 Awb een ander terrein dan artikel 13 Grondwet. Enerzijds kan artikel 13 Grondwet dus niet worden tegengeworpen aan de plicht tot medewerking van de verzender en ontvanger bij het verschaffen van zakelijke gegevens en bescheiden in het kader van het toezicht op de naleving. Uiteraard zijn toezichthouders alleen gerechtigd deze bevoegdheden uit te oefenen voor zover dat voor de vervulling van hun taak redelijkerwijs nodig is en met inachtneming van de wettelijke eisen die daaraan worden gesteld. Anderzijds geeft artikel 5:17 Awb niet de bevoegdheid tot het vorderen van inzage in persoonlijke of zakelijke communicatie bij een derde die de communicatie beheert, zonder de door artikel 13 Grondwet vereiste machtiging, nu hierbij het te beschermen rechtsbelang van artikel 13 in het geding is. Kort gezegd valt het vorderen van inzage van communicatie die aanwezig is bij de verzender of de geadresseerde niet onder de bescherming van artikel 13. Het vorderen van inzage in communicatie bij een derde die de communicatie beheert, die niet voor die derde is bestemd of van hem afkomstig is, valt wel onder de bescherming van artikel 13.

[88] Kamerstukken II 1993/94, 23 700, nr. 3, blz. 144.

Bijzondere wetgeving bevat vergelijkbare verplichtingen tot het desgevraagd verstrekken van gegevens en inlichtingen en het beschikbaar stellen van boeken en bescheiden (waaronder begrepen digitale opslag daarvan) die van belang kunnen zijn voor een goede taakuitoefening, bijvoorbeeld aan de inspecteur van de rijksbelastingdienst voor de juiste belastingheffing (artikelen 47 en 52 van de Algemene wet inzake rijksbelastingen) of aan de douane (artikel 14 Communautair douanewetboek[89], al dan niet in samenhang met artikel 1:5 van de Algemene douanewet). Voor de verhouding van deze specifieke wetsbepalingen tot artikel 13 Grondwet geldt hetzelfde als hiervoor is opgemerkt voor de verhouding tussen artikel 13 en titel 5.2 van de Awb.

5.5. Telecommunicatiewet

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.
Artikel 18.13, eerste lid, Tw bepaalt dat 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 communicatietechnieken in acht moeten worden genomen. Het tweede lid 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.
Artikel 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 over een elektronisch communicatienetwerk of voor de facturering daarvan».[90] 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 artikel 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

[89] Verordening (EEG) nr. 2913/92 van de Raad van 12 oktober 1992 tot vaststelling van het communautair douanewetboek (PbEG 1992, L 302). De grenzen van deze bevoegdheid wordt ingegeven door de eis van proportionaliteit, welke volgt uit artikel 1:21 Algemene douanewet en jurisprudentie van het Hof van Justitie van de Europese Unie, arrest van 19 januari 1980, 41/79 (Testa).
[90] Artikel 11.1 sub b Tw.

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 artikel 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. In het Wetboek van Strafvordering en de Wiv 2002 zijn regels opgenomen over de toegang tot deze gegevens ten behoeve van de opsporing en vervolging van strafbare feiten en de uitvoering van de wettelijke taken van de inlichtingen- en veiligheidsdiensten. 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.[91]
Tot slot kan artikel 11.2a Tw niet onvermeld blijven. 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.[92] 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 Autoriteit Consument en Markt (hierna: ACM) 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 persoonlijke levenssfeer.
Net als in het Wetboek van Strafrecht zijn aldus ook bepalingen in de Tw opgenomen die erop zijn gericht te voorkomen dat de aanbieder van communicatiediensten inbreuk maakt op het telecommunicatiegeheim.[93] De huidige Telecommunicatiewet verhoudt zich goed tot het voorstel voor het nieuwe artikel 13. 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, met uitzondering van het nog niet in werking getreden artikel 13.7 Tw.[94] Als deze laatste bepaling in werking treedt kan, zoals het agentschap Telecom heeft opgemerkt, ook voor niet-openbare telecommunicatiediensten de verplichting gaan gelden dat deze in het belang van de veiligheid van de staat of de handhaving van de strafrechtelijke rechtsorde aftapbaar moeten zijn. Gesloten communicatienetwerken worden thans bestreken door de Wbp en de relevante bepalingen in het Burgerlijk Wetboek. De

---

[91] Artikelen 126n/u, 126na/ua, 126nb/ub, 126ng/ug, 126zh tot en met 126zj, en 126hh Sv en artikelen 28 en 29 Wiv 2002.
[92] Artikel 11.2a implementeert artikel 5, eerste en tweede lid van de ePrivacyrichtlijn.
[93] Vgl. artikelen 139c en 273d Sr.
[94] Sommige gesloten netwerken vallen eveneens onder de reikwijdte van de Tw, bijvoorbeeld het vergunningvrij frequentiegebruik door basisstations met bijbehorende telefoons voor onder meer netwerken van werkgevers (artikel 3.4 lid 1 sub a Tw, jo. artikel 2, lid 2 sub o en artikel 8a van de Regeling gebruik van frequentieruimte zonder vergunning 2008).

voorgestelde grondwetsbepaling heeft een ruimere reikwijdte dan de meeste bepalingen in de Tw, die voor het overgrote deel slechts zien op openbare telecommunicatienetwerken en niet op (buitenlandse) aanbieders van een dienst informatiemaatschappij, zoals webmail-diensten.[95] Dat betekent dat inzage in privé-communicatie door de overheid alleen mogelijk is onder de voorwaarden die artikel 13 daaraan stelt, ongeacht de soort aanbieder van een communicatiedienst. In hoeverre het gewenst is ook in horizontale relaties de verplichtingen voor telecommunicatieaanbieders verder te laten reiken dan in de huidige Tw – zodat begrippen uit de Grondwet en de Tw een vergelijkbare interpretatie en reikwijdte krijgen – is een afweging die door de wetgever zal moeten worden gemaakt als het onderhavige voorstel tot wijziging van artikel 13 tot wet is verheven.

5.6. Postwet 2009

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. De Postwet 2009 is van toepassing op alle postvervoer met uitzondering van (a) het vervoer van afzonderlijk geregistreerde exprespost en (b) het vervoer van post door een derde naar het postvervoerbedrijf dat zorg draagt voor de daadwerkelijke bezorging op een adres (artikel 2, tweede lid, onderdelen a en b, van de Postwet 2009).
Artikel 4 van de Postwet 2009 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. Hoe bedrijven hieraan invulling geven wordt overgelaten aan de bedrijven zelf om onnodige belemmeringen in de bedrijfsvoering te voorkomen. De ACM ziet er op toe dat postvervoerbedrijven deze plicht naleven.
Op grond van artikel 5 van de Postwet 2009 is voorts bepaald dat het openen van onbestelbare post door een postvervoerbedrijf alleen is 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.

6. Administratieve lasten en uitvoeringskosten

Uit dit wetsvoorstel tot wijziging van artikel 13 van de Grondwet vloeien geen zelfstandige administratieve lasten voort. Voor zover er aanpassingswetgeving nodig is om de lagere regelgeving in overeenstemming te brengen met de Grondwet, waar wel administratieve lasten aan zijn verbonden, worden deze in kaart gebracht bij de betreffende wetgeving.

[95] Artikel 11.7a Tw richt zich anders dan de overige bepalingen van de Tw ook tot anderen dan aanbieders van elektronische communicatiediensten of -netwerken, zoals websitehouders, namelijk tot een ieder die informatie plaatst of leest op een randapparaat van een gebruiker van een elektronische communicatiedienst.

II. ARTIKELSGEWIJZE TOELICHTING

Artikel II (nieuw artikel 13)

Het eerste lid

Hiervoor wordt verwezen naar paragraaf 2 van het algemeen deel van de toelichting. 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. De keuze voor twee afzonderlijke leden, in plaats van in hetzelfde lid zowel het communicatiegeheim als de daarop toegestane beperkingen op te nemen, zoals in het huidige artikel 13 het geval is, betreft een wetgevingstechnische keuze, die op zichzelf niet leidt tot een verruiming van de toegestane beperkingen. Er is voorts in aansluiting op artikel 10 Grondwet gekozen voor de term eerbiediging in plaats van de wat oudere term onschendbaarheid. Daarmee is geen wijziging beoogd in het karakter van het grondrecht of de mate van rechtsbescherming die het biedt, ten opzichte van het huidige artikel 13. Het eerste lid is in rechte inroepbaar en geeft een onthoudingsplicht voor de overheid aan.

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. Wij volgen de staatscommissie hierin en kiezen voor de term machtiging.

De zinsnede «door of met machtiging hen die daartoe bij de wet zijn aangewezen» biedt een duidelijke basis voor zowel de mogelijkheid dat de wet zelf de functionaris aanwijst die inbreuk mag maken op het brief- en telecommunicatiegeheim, als voor de mogelijkheid dat de wetgever een functionaris aanwijst die bevoegd is om anderen te machtigen dergelijke inbreuken te maken. Deze uitleg sluit qua systematiek aan bij de uitleg van de grondwetgever van 1983 van het huidige tweede lid van artikel 13[96], dat beperkingen door of met machtiging van hen die daartoe bij wet zijn aangewezen mogelijk maakt.

Artikel III (additioneel artikel)

Het 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 maakt het mogelijk bestaande beperkingen die in strijd zijn met het nieuwe artikel in overeenstemming te brengen met het nieuwe artikel. Zoals is toegelicht in paragraaf 5 van het algemene gedeelte van deze toelichting, voorziet de huidige wetgeving voor het overgrote deel, ook met

[96] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 45.

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.

De Minister-President, Minister van Algemene Zaken,
M. Rutte

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk

De Minister van Veiligheid en Justitie,
I.W. Opstelten