Datum
20 DEC. 2012
Van
Uw kenmerk:
2012-0000594436

Ons kenmerk:
SBK/86613/IZ

Postbus 58285, 1040 HG Amsterdam

De Minister van Binnenlandse Zaken en Koninkrijksrelaties
De heer dr. R.H.A. Plasterk
Postbus 20011
2511 EG DEN HAAG

Onderwerp:
Consultatie conceptwetsvoorstel tot wijziging van artikel 13 Grondwet

Geachte heer Plasterk,

Met uw brief van 9 november 2012 heeft u ons in de gelegenheid gesteld om te reageren op het conceptwetsvoorstel tot wijziging van artikel 13 van de Grondwet.

Wij danken u voor de door u geboden gelegenheid om de voorgenomen wijziging van artikel 13 Grondwet te toetsen op mogelijke consequenties voor UWV.

In uw bovenvermelde brief heeft u ons expliciet gevraagd om aan twee elementen in het conceptwetsvoorstel specifiek aandacht te besteden.
Het betreft in de eerste plaats een antwoord op de vraag of het achterwege laten van een machtiging van de rechter om het brief- en telecommunicatiegeheim te beperken en te vervangen door een machtiging van één of meer bij wet aangewezen ministers gevolgen heeft voor de werkwijze van onze organisatie.
In de tweede plaats wordt ons gevraagd of wij meerwaarde zien in het bepaalde in lid 3 van artikel 13 Grondwet om regels te stellen ter bescherming van het brief- en telecommunicatiegeheim.

Uitvoeringsconsequenties
Onze conclusie is dat de wijziging van artikel 13 Grondwet geen specifieke wijzigingen in de uitvoeringspraktijk voor UWV met zich meebrengt.

Op uw vraag of de wijziging leidt tot een andere werkwijze door UWV het volgende.
Verzoeken om gegevens te leveren op basis van een machtiging van een rechter worden ingediend bij UWV. Dit verandert ook niet door de wijziging van artikel 13 GW.
Na de wijziging van artikel 13 Grondwet kunnen de machtigingen van de daartoe door de wet aangewezen minister(s) eveneens aan UWV worden gericht.
Voor UWV moet dan wel onomstotelijk vast staan en duidelijk zijn dat het een 'machtiging' is van een daartoe bij wet aangewezen minister, dat het verzoek om levering van gegevens betrekking heeft op een beperking van het brief- en telecommunicatiegeheim en dat de 'machtiging' is afgegeven in het belang van de nationale veiligheid. UWV zal dan ook de interne instructies op dat punt aanpassen.

Ook is onze inschatting dat de wijziging van artikel 13 GW niet tot een uitbreiding van het aantal verzoeken om levering van gegevens zal leiden, maar een inschatting vooraf is moeilijk te maken.

Op uw vraag of UWV voordelen ziet in de mogelijkheid voor de wetgever om nadere regels te treffen (zoals voorzien in lid 3 van het nieuwe artikel 13 GW) is ons antwoord dat wij deze vooralsnog niet zien.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

mr. drs. B.J. Bruins
Voorzitter Raad van Bestuur

cc de minister van Sociale Zaken en Werkgelegenheid, de heer mr. dr. L.F. Asscher

Postbus 90420
2509 LK Den Haag
Telefoon (070) 315 35 00
Fax (070) 315 35 01
E-mail mail@opta.nl
www.opta.nl

Bezoekadres
Zurichtoren
Muzenstraat 41
2511 WB Den Haag

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011
2500 EA 'S-GRAVENHAGE

Contactpersoon	Ons kenmerk	Uw kenmerk	Doorkiesnummer
ir	OPTA/AM/2012/203050	2012-0000581107	
Datum	**Onderwerp**		**Bijlage(n)**
19 DEC. 2012	12.0200.01 Consultatie conceptwetsvoorstel tot wijzinging van artikel 13 Grondwet		1

Geachte heer, mevrouw

Bij brief van 16 oktober 2012, met opgemeld kenmerk, heeft u het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna; het college) uitgenodigd om een reactie te geven op het conceptvoorstel tot wijzing van artikel 13 van de Grondwet.

In bijgevoegd document doet het college u zijn reactie toekomen.

Het college heeft geen bezwaar tegen openbaarmaking van het document. Het document is daartoe ook geüpload naar de website Internetconsultatie.

Een afschrift van deze reactie zendt het college toe aan het Ministerie van Economische Zaken.

Hoogachtend,

HET COLLEGE VAN DE ONAFHANKELIJKE POST EN TELECOMMUNICATIE AUTORITEIT,
namens het college,
Plv. afdelingshoofd afdeling Markten

ir. M.G.J. Meijers

OPTA

Ons kenmerk: OPTA/AM/2012/203049
Zaaknummer: 12.0200.01
Datum: 19 DEC. 2012

Reactie van het college van de Onafhankelijke Post en Telecommunicatie Autoriteit op het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet

1 Inleiding

Bij brief van 16 oktober 2012, met kenmerk 2012-0000581107, heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: het college) uitgenodigd om een reactie te geven op het conceptvoorstel tot wijzing van artikel 13 van de Grondwet. Bij brief van 2 november 2012, met kenmerk WJZ/12349286, attendeert het ministerie van Economische Zaken de diverse uitvoeringsinstanties op het gebied van EZ op het conceptvoorstel en geeft daarbij aan dat de wetswijziging mogelijk gevolgen heeft voor de uitoefening van de taken, waardoor noodzaak wordt gezien om op het conceptvoorstel te reageren.

Het college zal in zijn reactie op het conceptvoorstel aandacht schenken aan de in dit artikel opgenomen regelingsopdracht aan de wetgever. Het college zal verder een aantal risico's en aandachtspunten aangeven vanuit zijn expertise op grond van toezicht en handhaving van bescherming van het brief- en telecommunicatiegeheim in de Postwet 2009 (hierna: Pw) en de Telecommunicatiewet (hierna:Tw).

2 Het voorgestelde artikel 13 Grondwet

Het college is van mening dat modernisering in de vorm van een techniekonafhankelijke invulling van de bescherming van het communicatiegeheim, in het voorgestelde artikel 13 van de Grondwet neergelegd als bescherming van het brief en telecommunicatiegeheim, een adequate reactie is op de ontwikkelingen in het digitale tijdperk.

Het college ziet de meerwaarde van het derde lid van het voorgestelde artikel 13 Grondwet, waarin een regelingsopdracht voor de wetgever is opgenomen waarmee de bescherming van het brief- en telecommunicatiegeheim in private verhoudingen, mede met het oog op mogelijke ontwikkeling van nog onbekende communicatiemiddelen en technieken, tot aanhoudende zorg voor de overheid wordt verklaard. Door privatisering, liberalisering en convergentie van communicatiemiddelen is het stellen van wettelijke regels waarin verplichtingen worden opgelegd noodzakelijk om het brief- en telecommunicatiegeheim te waarborgen. De burger moet de verzending en bezorging van zijn communicatie aan private partijen toevertrouwen, terwijl het hem vaak aan kennis en middelen ontbreekt om zelf de vertrouwelijkheid van zijn communicatie te beschermen.

3 Borging van het brief en telecommunicatiegeheim in Pw en Tw

In het kader van de regelingsopdracht aan de wetgever vermeldt de toelichting bij het voorliggende conceptwetsvoorstel de reeds in de artikelen 4 tot en met 6 van de Pw en in artikel 18:13 van de Tw

uitgewerkte borging van het grondrechtelijk belang van bescherming van het brief- en telecommunicatiegeheim. Het college zal daar hieronder op ingaan.

3.1 De borging van het briefgeheim in de Pw

Wat betreft de borging van het briefgeheim in artikel 4 van de Pw, merkt het college het volgende op. Dit artikel verplicht de postvervoerbedrijven om bij het uitvoeren van hun postvervoerdiensten schending van het grondwettelijk briefgeheim te voorkomen. Het college dient er vervolgens op toe te zien dat een postbedrijf voldoende maatregelen heeft genomen om het briefgeheim te waarborgen.

Het college merkt op dat artikel 4 van de Pw volgens de memorie van toelichting bij het conceptwetsvoorstel artikel 13 Grondwet onder meer inhoudt dat maatregelen moeten worden genomen om ervoor te zorgen dat sorteercentra niet voor een ieder toegankelijk zijn. In de memorie van toelichting bij de Postwet 2009 staat echter dat de wijze waarop bedrijven invulling geven aan de verplichting om schending van het briefgeheim te voorkomen, wordt overgelaten aan de bedrijven zelf om onnodige belemmeringen in de bedrijfsvoering te voorkomen. Het college constateert dat de memorie van toelichting bij het conceptwetsvoorstel artikel 13 Grondwet stringenter is dan de memorie van toelichting bij artikel 4 van de Pw beoogt. Zo staat in de toelichting bij de Pw dat postvervoerbedrijven er voor moeten zorgen dat derden niet in de gelegenheid zijn het briefgeheim te schenden, maar alleen voor zover het redelijkerwijs in de macht van het bedrijf ligt om schending van het briefgeheim te voorkomen.

Als de grondwetgever, wellicht mede in het licht van het toenemend aantal berichten over gevallen waarin de kwaliteit van het postvervoer te wensen overlaat, een stringentere bescherming van het briefgeheim wenselijk acht, dan ligt het naar het oordeel van het college in de rede om de Pw op dit punt te herijken.

3.2 De borging van het telecommunicatiegeheim in de Tw

Volgens de memorie van toelichting bij het conceptvoorstel verhoudt de huidige Tw zich goed tot het voorstel van het nieuwe artikel 13 Grondwet en geeft deze reeds uitvoering aan de regelingsopdracht in het derde lid. De memorie van toelichting vermeldt hierbij artikel 18:13 Tw dat ertoe strekt de bescherming van de privacy en het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken in de Tw te verankeren. De toelichting vermeldt verder de bescherming van persoonsgegevens en de persoonlijke levenssfeer op grond van een aantal artikelen in hoofdstuk 11 van de Tw. In de toelichting bij het conceptvoorstel wordt geconcludeerd dat deze bepalingen in de Tw wat betreft de openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten een groot deel van de lacunes in de bescherming van het brief- en telecommunicatiegeheim in horizontale verhoudingen vullen.

Het college onderschrijft dat het stelsel van wettelijke bepalingen in hoofdstuk 11 van de Tw (o.a. artikel 11.2a Tw) en artikel 18.13 Tw een groot deel invult van de bescherming van het brief- en telecommunicatiegeheim in horizontale verhoudingen bij openbare elektronische communicatiediensten en -netwerken. Tegelijkertijd acht het college het aannemelijk dat het stelsel van hoofdstuk 11 Tw en artikel 18.13 Tw verdere herformulering of invulling behoeft om aan de strekking van artikel 13 Grondwet invulling te geven; de in de memorie van toelichting gehanteerde voorbeelden, zoals bijvoorbeeld ten aanzien van social media, zijn technologisch actueler dan die in de Telecommunicatiewet.

Ten aanzien van artikel 18:13 Tw merkt het college daarnaast op dat dit artikel in 1998 bij amendement in de Tw is geïntroduceerd.[1] Volgens de toelichting strekt het amendement ertoe de bescherming van de privacy en het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken zoals fax en e-mail in de Tw te verankeren. Het wetsvoorstel tot wijziging van artikel 13 van de Grondwet dat hiervoor de aanleiding vormde[2], is gesneuveld, maar het bij amendement voorgestelde artikel 18.13 Tw is ongewijzigd in de Tw opgenomen.

Gelet op het vorenstaande adviseert het college de wetgever om de terminologie en formulering van artikel 18:13 Tw nader te bezien en om eventuele lacunes in hoofdstuk 11 Tw en artikel 18.13 Tw in te vullen om zodoende interpretatieverschillen tussen de Tw en artikel 13 Grondwet te voorkomen.

4 Risico's en aandachtspunten

Het college zou hieronder graag nog een aantal risico's en aandachtspunten willen aangeven die hij ziet bij het conceptvoorstel.

4.1 Verkeersgegevens

Verkeersgegevens die niet mede betrekking hebben op de inhoud van de communicatie, vallen volgens de memorie van toelichting buiten de bescherming van het grondwetsartikel.

Het college wijst er in dit verband op dat de technologische ontwikkelingen een strikte scheiding tussen inhoud- en verkeersgegevens problematisch maken. Terecht wordt op dit punt ingegaan aan het slot van paragraaf 2.3 van de memorie van toelichting. Als een gebruiker bijvoorbeeld de inhoud van een bepaalde webpagina ophaalt, dan is die inhoud de communicatie en is de URL die de gebruiker daartoe intoetst een verkeersgegeven. Als de gebruiker echter een zoekopdracht in een zoekmachine opgeeft, dan wordt de zoekopdracht in de URL opgenomen en naar de zoekmachine gestuurd. De URL is dan niet alleen een verkeersgegeven maar ook een deel van de inhoud van de communicatie.

Daarnaast merkt het college op dat het grondwetsvoorstel op dit punt niet aansluit bij de ontwikkelingen op internationaal gebied. Zo heeft het Europees Hof voor de Rechten van de Mens in zijn jurisprudentie over artikel 8 van het Europees Verdrag voor de Rechten van de Mens (zie bijvoorbeeld de zaken *Malone*[3] en *P.G. & J.H.*[4]) erkend dat verkeersgegevens een onlosmakelijk onderdeel uitmaken van de door artikel 8 EVRM beschermde communicatie. Ook de ePrivacyrichtlijn gaat er vanuit dat de communicatie en de daarmee verband houdende verkeersgegevens onlosmakelijk met elkaar zijn verbonden.[5]

---

[1] Tweede Kamer, vergaderjaar 1997–1998, 25 533, nr. 75

[2] Handelingen II 1996/1997, nr. 1370

[3] EHRM 2 augustus 1984, Series a.82 (Malone).

[4] EHRM 25 september 2001, NJ 2003, 670, m.nt. E. J. Dommering (*P.G. & J.H.*)

[5] Zie bijvoorbeeld overweging 21 ePrivacyrichtlijn: *"Er moeten maatregelen worden getroffen om onbevoegde toegang tot communicatie te verhinderen, teneinde het vertrouwelijke karakter van communicatie via openbare elektronische-communicatienetwerken en openbare elektronische-diensten te beschermen, zowel ten aanzien van de inhoud zelf als van*

Gelet op het vorenstaande adviseert het college nadere aandacht te geven aan dit afbakeningsprobleem tussen verkeersgegevens en inhoudsgegevens bij uitwerking van het brief- en telecommunicatiegeheim in de (lagere) wet- en regelgeving.

4.2 Feitelijke beschikkingsmacht van de derde over de communicatie

Volgens de memorie van toelichting bij het conceptvoorstel is de bescherming van het brief- en telecommunicatiegeheim aan de orde zolang de communicatie in de feitelijke beschikkingsmacht van de derde is.

Het college wijst er op dat een aanbieder ook een andere partij kan inschakelen voor het verrichten van werkzaamheden. De communicatie is dan niet in de feitelijke beschikkingsmacht van de aanbieder en deze kan daardoor zelf geen effectieve bescherming bieden. Naar het oordeel van het college is het aangewezen dat de aanbieder zelf verantwoordelijk blijft voor de dienstverlening en voor de naleving van de wettelijke verplichtingen daarbij. De aanbieder dient dan afspraken te maken met de uitvoerder van werkzaamheden teneinde deze verplichtingen te waarborgen. Een toezichthouder moet de betrokken aanbieder kunnen aanspreken op zijn verantwoordelijkheid als de wettelijke verplichting wordt geschonden.

Het college verwijst hierbij naar het nieuwe artikel 11.2a Tw, tweede lid, en de daarbij behorende toelichting waarin het vorenstaande eveneens is neergelegd. Het Hof van Justitie heeft in het arrest van 22 november 2012 geoordeeld dat als in de telecommunicatiesector de verwerking van persoonsgegevens wordt uitbesteed, dan in de uitbestedingovereenkomst daarover dan clausules moeten staan. De uitbestedende partij kan dan controleren of het privacyrecht wordt nageleefd.[6] Deze internationale ontwikkeling, in het arrest betreffende verkeersgegevens, ondersteunt het belang van de juridische beschikkingsmacht als criterium voor bescherming.

Het college adviseert om de bescherming van het brief- en telecommunicatiegeheim zich in de wetgeving te laten uitstrekken tot de juridische beschikkingsmacht van de derde. Als de derde een andere partij inschakelt voor het verrichten van werkzaamheden, dan blijft hij zelf verantwoordelijk voor de dienstverlening en voor de naleving van de wettelijke verplichtingen daarbij. Om deze verplichtingen te waarborgen moet de derde dan afspraken maken met de uitvoerder van werkzaamheden.

4.3 Informed consent

In paragraaf 4.1 van de memorie van toelichting bij het conceptwetsvoorstel staat dat instemming van de gebruiker over het inzien van communicatie vaak zal geschieden door aanvaarding van de algemene voorwaarden (informed consent) van een bedrijf. Volgens de wetgever kan het in de toekomst nodig zijn dat hij de burger ondersteunt met bepaalde effectieve rechten voor de burger en

---

gegevens over de communicatie. De nationale wetgeving van sommige lidstaten verbiedt uitsluitend opzettelijk onbevoegde toegang tot communicatie." Zie ook artikelen 5 en 6 van de genoemde richtlijn.

[6] Intellectuele eigendom & IT-recht, Dirkzwager advocaten - Hof van Justitie dwingt controlemechanismes af in bewerkersovereenkomst

plichten van de bedrijven. Dit omdat contractuele afspraken niet altijd een goed geïnformeerde beslissing van de gebruiker waarborgen.

Vanuit zijn ervaring uit de toezichtpraktijk met het spam- en spyware-verbod kan het college bevestigen dat toestemming een moeilijk toe te passen leerstuk is, met name als dit is opgenomen in de algemene voorwaarden. Bij toestemming moet sprake zijn van een vrije, specifieke en op informatie berustende wilsuiting. Het ondertekenen van algemene voorwaarden, die van toepassing zijn op het sluiten van een overeenkomst, wil niet automatisch zeggen dat er daadwerkelijk sprake is van dergelijke toestemming als bedoeld in artikel 1, onder i van de Wet bescherming persoonsgegevens.[7]

Het college adviseert om het vorenstaande op te nemen in de desbetreffende passage in de memorie van toelichting bij artikel 13 Grondwet.

5 Overleg over aandachtpunten

Het college gaat graag met de wetgever in gesprek over de in zijn reactie vermelde (aandacht)-punten, met name ten behoeve van uitwerking van het brief- en telecommunicatiegeheim in de wet- en regelgeving die gerelateerd is aan de bevoegdheden van het college.

HET COLLEGE VAN DE ONAFHANKELIJKE POST EN TELECOMMUNICATIE AUTORITEIT,
namens het college,

mr. C.A. Fonteijn, voorzitter

[7] *Handelingen I*, 1999-2000, nr. 34, p. 1632.

Nederlands Juristen Comité voor de Mensenrechten
Dutch section of the International Commission of Jurists

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Plaatsvervangend directeur Constitutionele Zaken en Wetgeving

Postbus 20011
2500 EA Den Haag

Leiden, 20 december 2012

Betreft: Consultatie conceptwetsvoorstel tot wijziging van artikel 13 Grondwet

Geachte heer Pedroli,

Bij brief d.d. 16 oktober 2012 nodigde u het Nederland Juristen Comité voor de Mensenrechten (NJCM) uit om een reactie te geven op het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet. In het bijzonder vroeg u om de visie van het NJCM op de meerwaarde van de voorgestelde regelingsopdracht in het derde lid van artikel 13 Grondwet. Het NJCM komt bij dezen graag aan uw uitnodiging tegemoet.

Inhoud en reikwijdte

Dat het huidige artikel 13 van de Grondwet aan modernisering toe is, wordt zonder meer door het NJCM onderkend. Met het voorgestelde artikel is de wetgever bovendien een stap verder gegaan, door te streven naar een volledig techniekonafhankelijke benadering waarmee zowel huidige als toekomstige communicatiemiddelen bescherming zouden moeten genieten. Met de overstap van brief-, telefoon- en telegraafgeheim naar brief- en telecommunicatiegeheim is dit naar het oordeel van het NJCM gelukt. Temeer door de ruime interpretatie die in de memorie van toelichting (MvT) wordt toegekend aan telecommunicatie (het overbrengen van informatie op afstand, ongeacht de gebruikte overdrachtsmiddelen). Ook ziet het NJCM meerwaarde in de uitbreiding van bescherming louter in de transportfase naar bescherming tijdens tussentijdse opslag.

De wetgever heeft een afbakening aan de hand van drie criteria voorgesteld: de aanwezigheid van een communicatiemiddel, betrokkenheid van een derde en gerichtheid van de communicatie. Hoewel het begrip 'derde' wellicht nadere toelichting vraagt, wekt de betreffende afbakening op het eerste gezicht de indruk zowel logisch als werkbaar te zijn.

Op inhoud en op reikwijdte ondersteunt het NJCM de gekozen benadering bij het voorgestelde artikel 13 Grondwet. Desalniettemin stelt het NJCM kritische vragen op enkele onderdelen die hieronder uiteengezet worden.

Beperkingen: rechtelijke machtiging als hoofdregel

In het voorgestelde artikel 13 Grondwet wordt de bescherming van het brief- en telecommunicatiegeheim gelijkgesteld aan de bescherming die nu voor het briefgeheim geldt: beperking van het grondrecht is slechts mogelijk met een voorafgaande machtiging van de rechter. Het NJCM staat positief tegenover dit door de wetgever gekozen beschermingsniveau, waarmee de wetgever aansluiting lijkt te hebben gezocht bij de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM).

Het verdient evenwel aanbeveling om in de MvT nader uit te werken welk toetsingskader de wetgever voor ogen heeft voor de rechter bij het geven van toestemming op inbreuken op het grondrecht. Conform jurisprudentie van het EHRM dienen inbreuken te worden getoetst aan de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit. De motivering van de inbreuk dient te zijn toegespitst op de concrete omstandigheden van het geval en de beschikbare relevante informatie dient hierbij te worden betrokken. Door het toetsingskader nader uit te werken wordt een ijkpunt gegeven voor de praktijk, hetgeen de waarborgfunctie van de Grondwet versterkt.

Beperkingen: afwijking van hoofdregel in het kader van de nationale veiligheid

Op bovengenoemde hoofdregel wordt in het voorgestelde artikel 13 Grondwet direct een uitzondering gecreëerd. In het kader van de nationale veiligheid is het niet de rechter maar de minister die de toestemming mag geven voor de beperking van het brief- en telecommunicatiegeheim. Hoewel deze uitzondering in lijn is met de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (Wiv 2002), plaatst het NJCM enkele kanttekeningen hierbij.

In de MvT wordt toegelicht dat de voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) of de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) verantwoordelijke Minister beter geïnformeerd is dan een rechter om de afweging te maken of beperking van het brief- en telecommunicatiegeheim gerechtvaardigd is. Ook zou deze afweging vaak politiek-bestuurlijk van aard zijn. Het NJCM betwijfelt sterk of dit het geval is. Bij de inzet van de afluisterbevoegdheid door de AIVD (artikel 25 Wiv 2002) bijvoorbeeld, gaat het om grote hoeveelheden operaties. De Minister van BZK heeft geen ambtelijke ondersteuning bij het maken van deze afweging, maar wordt direct door het hoofd van de AIVD geïnformeerd.[1] Het is de vraag in hoeverre de minister tijd heeft voor een grondige individuele afweging. Bovendien ziet de te maken afweging eerder op rechtmatigheid dan op politiek-bestuurlijke wenselijkheid. De AIVD dient overtuigend te motiveren dat een inbreuk op het brief- en telecommunicatiegeheim noodzakelijk, proportioneel en subsidiair is. De afweging of deze inbreuk gerechtvaardigd is, verdient een onafhankelijk juridisch oordeel, niet zozeer een politiek-bestuurlijk oordeel.

Het blijkt daarnaast duidelijk uit de rechtspraak van het EHRM dat het de sterke voorkeur geniet om inbreuken op het brief- en telecommunicatiegeheim slechts plaats te laten vinden na toestemming van een onafhankelijke derde. Dit geldt niet alleen in het kader van de opsporing, maar ook in het kader van het werk van inlichtingen- en veiligheidsdiensten.[2] Recentelijk nog benadrukte het EHRM in een zaak tegen Nederland het belang van een voorafgaande toets van een onafhankelijke derde bij de inzet van bijzondere bevoegdheden.[3]

In enkele andere Europese landen, bijvoorbeeld België en Duitsland, is een dergelijke onafhankelijke toets voorafgaande aan de inzet van bijzondere bevoegdheden gebruikelijk. Het blijkt wel degelijk mogelijk om voorafgaand aan deze inzet *checks en balances* te introduceren. Het verdient aanbeveling om deze mogelijkheden te verkennen, in plaats van ze bij voorbaat uit te sluiten.

---

[1] C. Fijnaut, *Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel*, p. 94, www.ctivd.nl.

[2] EHRM 6 september 1978 (Klass/Duitsland), §§ 21, 51 en 56; EHRM 29 juni 2006 (Weber en Saravia/ Duitsland), §§ 25 en 117; EHRM 18 mei 2010 (Kennedy/VK), §§ 56 en 57; EHRM 14 september 2010 (Sanoma/Nederland), §§ 96 - 99.

[3] EHRM 22 november 2012 (Telegraaf/Nederland), § 96 ev.

Beperkingen: mogelijkheid tot mandateren in het kader van de nationale veiligheid

In de MvT wordt vervolgens uitgelegd dat de minister de bevoegdheid om toestemming te geven voor een inbreuk op artikel 13 Grondwet niet mag delegeren maar wel mag mandateren. Het NJCM staat zeer kritisch tegenover de mogelijkheid van mandaat. Dit zou betekenen dat in de praktijk toestemming kan worden gegeven door het hoofd of een medewerker van de AIVD of de MIVD. Dit gebeurt weliswaar onder de verantwoordelijkheid van de minister, maar zonder diens betrokkenheid. Deze mogelijkheid is innerlijk tegenstrijdig met wat er eerder in de MvT wordt uitgelegd: als de uitvoerende macht zelf toestemming geeft voor een inbreuk op het brief- en telecommunicatiegeheim dan ontbreekt een natuurlijke drempel tegen willekeurig gebruik en ontbreken *checks and balances* (paragraaf 3.2).

En hoewel in de MvT wordt benadrukt dat aansluiting is gezocht bij de bestaande praktijk, betekent de algemene mogelijkheid van mandaat een afwijking van het regime van de Wiv 2002. Bij de totstandkoming van de Wiv 2002 is er immers voor gekozen om niet te voorzien in een mandaatregeling bij de bijzondere bevoegdheden die inbreuk maken op onder meer het telefoon- en telegraafgeheim. Dit betekent dat voor de inzet van de afluisterbevoegdheid en de selectie van Sigint op grond van de artikelen 19 j° 25 en 27 Wiv 2002 uitsluitend de verantwoordelijke minister bevoegd is om aan de AIVD en de MIVD toestemming te geven om te tappen. De minister mag deze taak niet mandateren.

Bovendien verhoudt deze mogelijkheid zich slecht tot de jurisprudentie van het EHRM. Als het verlenen van toestemming voor de inbreuk op het brief- en telecommunicatiegeheim in de praktijk in handen komt te liggen van de AIVD en de MIVD dan kan niet meer worden gesproken van een significante waarborg tegen misbruik van bevoegdheden.

Regelingsopdracht: ontbreken van notificatieplicht

De wetgever heeft in het huidige wetsvoorstel geen expliciete notificatieplicht opgenomen. Er is enkel een algemene regelingsopdracht in het derde lid van het voorgestelde artikel 13 Grondwet. Hiermee wordt het aan de formele wetgever overgelaten om de notificatieplicht al dan niet te regelen. Blijkens de MvT is voor deze weg gekozen, omdat de formele wetgever het beste kan afwegen en kan bepalen wanneer een notificatieplicht meerwaarde heeft voor het Nederlandse systeem van rechtsbescherming.

Volgens het NJCM is de notificatieplicht zowel voor opsporingsdiensten als voor inlichtingen- en veiligheidsdiensten een extra stok achter de deur om zich strikt aan de regels te houden bij het toepassen van verregaande inbreuken op de privacy zoals de inzet van de afluisterbevoegdheid. Immers, de strekking van de notificatieplicht is het bieden van (rechts)bescherming tegen overheidsoptreden dat inbreuk maakt op grondrechten van burgers. In deze bescherming (de zogenaamde *effective remedy* zoals neergelegd in artikel 13 van het Europees Verdrag voor de Rechten van de Mens (EVRM)) wordt voorzien door een betrokkene achteraf mede te delen welke opsporingsbevoegdheden jegens hem/haar zijn toegepast.

De notificatieplicht wordt ook door het EHRM gezien als een belangrijke, zo niet onmisbare waarborg tegen misbruik van deze bijzondere bevoegdheden.[4] In zowel de WIV 2002[5] als in het Wetboek van Strafvordering[6] is deze plicht opgenomen. Ook in artikel 12 Grondwet is de notificatieplicht expliciet opgenomen.

---

[4] Zie o.a. EHRM 6 september 1978 (Klass/Duitsland), § 57; EHRM 29 juni 2006 (Weber en Saravia/Duitsland), §135, EHRM 28 juni 2007 (Association for European Integration and Human Rights en Ekimdzhiev/Bulgarije), §§90-91, 101.

[5] Artikel 34 Wiv 2002.

[6] Ingevolge artikel 126bb Sv dient de officier van justitie aan betrokkene schriftelijk mededeling te doen van de uitoefening van de bevoegdheden, genoemd in de titels IVa tot en met Vc, zodra het belang van het onderzoek dat toelaat.

De MvT vermeldt dat de Staatscommissie Grondwet in 2010 de notificatieplicht niet heeft genoemd in haar advies. Dat zij deze geheel lijken te zijn vergeten, lijkt het NJCM geen reden om geen notificatieplicht in artikel 13 Grondwet op te nemen. De Commissie Franken heeft dit in 2000 wel geadviseerd.[7]

Concluderend adviseert het NJCM om de notificatieplicht wel expliciet in artikel 13 Grondwet te regelen. De Grondwet geeft op deze wijze voldoende invulling aan haar waarborgfunctie en aan de jurisprudentie van het EHRM.

Regelingsopdracht: horizontale verhoudingen

Afsluitend geeft het NJCM graag blijk van haar instemming met de keuze van de wetgever voor een regelingsopdracht in het wetsvoorstel ten behoeve van het waarborgen van het brief- en telecommunicatiegeheim in horizontale verhoudingen. Het NJCM bevestigt dat in de huidige samenleving de bescherming van het communicatiegeheim ten opzichte van de staat niet afdoende is. Door zowel technologische ontwikkelingen als de liberalisering van de telecommunicatie-infrastructuur en traditionele communicatiemiddelen hebben veel private partijen toegang tot of bezit over de communicatie tussen burgers. Deze private partijen kunnen met de informatie die zij op deze wijze vergaren een zekere macht uitoefenen over burgers die vergelijkbaar is met overheidsmacht. Het NJCM acht het dan ook nadrukkelijk van belang dat de overheid de bescherming van het communicatiegeheim in horizontale verhoudingen tot haar aanhoudende zorg rekent. Het past in de systematiek van de Grondwet om hiertoe de opdracht te geven.

Ook op internationaal niveau wordt het belang van bescherming van het communicatiegeheim in horizontale verhoudingen benadrukt. Dit volgt onder meer uit de toenemende positieve verplichtingen voortvloeiende uit artikel 8 EVRM en verschillende EU-richtlijnen.[8]

Gelet op het bovenstaande juicht het NJCM de voorgestelde constitutionele waarborg toe. Het NJCM ziet met verwachting uit naar het vervolg van het wetgevingstraject en wenst u hierbij veel succes.

Hoogachtend,

Friederycke Haijer
Voorzitter NJCM

[7] Rapport Commissie Grondrechten in het digitale tijdperk, 2000.

[8] Zie o.a. artikel 5 van Richtlijn 97/66/EG van het Europees Parlement en de Raad van de Europese Unie van 15 december 1997, artikel 2 onder 19 van Richtlijn 97/67/EG van het Europees Parlement en de Raad van de Europese Unie van 15 december 1997.

De Nederlandsche Bank
Eurosysteem

Juridische zaken

Postbus 98
1000 AB Amsterdam

tevens via
http://internetconsultatie.nl/briefentelecommunicatiegeheim/

De Minister van Binnenlandse Zaken en Koninkrijksrelaties

Postbus 20011
2500 EA DEN HAAG

Datum
28 december 2012
Uw kenmerk
--
Ons kenmerk
2012/677062
Behandeld door

Doorkiesnummer

Bijlage(n)
--

Onderwerp
reactie DNB op internetconsultatie wijziging artikel 13 Grondwet

Geachte heer Pedroli,

De Nederlandsche Bank N.V. (DNB) is u erkentelijk voor de geboden gelegenheid om een reactie te geven op het concept voor een voorstel van wet inzake de wijziging van artikel 13 van de Grondwet. DNB maakt bij het concept graag de volgende opmerkingen. De Autoriteit Financiële Markten (AFM) onderstreept deze opmerkingen.

U vroeg in het bijzonder om een reactie op twee vragen. De eerste vraag betrof de mogelijke gevolgen voor de werkwijze van DNB van het uitgangspunt dat voor beperkingen op het brief- en telecommunicatiegeheim in beginsel een machtiging van de rechter vereist is, met als uitzondering dat in het belang van de nationale veiligheid beperkingen zijn toegestaan met machtiging van één of meer bij wet aangewezen ministers.

Een beoordeling van de mogelijke gevolgen van de machtigingseis vereist allereerst een beoordeling van de reikwijdte van het gewijzigde grondrecht. DNB acht daarbij het volgende van belang.

Betrokkenheid van een derde
Ten eerste is van belang dat uit het concept voor de Memorie van Toelichting (MvT) volgt dat het brief- en telecommunicatiegeheim slechts aan de orde is indien drie cumulatieve criteria aan de orde zijn (p. 12). Eén van die criteria is de aanwezigheid van een derde die is belast met het beheer over de overdracht en/of opslag van de communicatie. Het huidige artikel 13, eerste lid, pleegt zo te worden uitgelegd dat het moet gaan om een brief die aan een derde is toevertrouwd (o.a. HR 18 oktober 1994, NJ 1995/101).

DNB is van mening dat de MvT bij dit criterium meer duidelijkheid zou kunnen bieden, vooral ten aanzien van communicatie zich in opslag bij een derde bevindt. In de MvT staat namelijk dat bescherming heeft te gelden zolang de derde feitelijk toegang heeft tot de inhoud van het bericht en dat het brief- en telecommunicatiegeheim aan de orde is zolang de communicatie in de feitelijke beschikkingsmacht van de derde is (p. 14). Tevens staat in de MvT de opmerking dat de

overheid "noch via de derde noch direct bij de verzender kennis mag nemen van de inhoud van een bericht zonder dat daarvoor een formeel wettelijke grondslag bestaat en er een rechterlijke machtiging is gegeven"(onderstreping DNB). Met het onderstreepte gedeelte lijkt gedoeld te worden op een situatie waarin een kopie van het bericht bij de verzender aanwezig is, hetgeen bij e-mail de gangbare praktijk is. De vraag doet zich dan voor of het tweede criterium (derde met beheer over overdracht en/of opslag) beperkter is geformuleerd dan dat de wetgever nu voor ogen staat.

Privé-communicatie
Een tweede aspect dat ziet op de reikwijdte van het grondrecht betreft het volgende. Enerzijds kan uit de MvT worden afgeleid dat het brief- en telecommunicatiegeheim ziet op privé-(persoonlijke) communicatie en niet op zakelijke communicatie. In de MvT staat namelijk dat het brief- en telecommunicatiegeheim een uitwerking is van één van de bijzondere aspecten binnen het recht op bescherming van de persoonlijke levenssfeer (p. 20) en dat artikel 13 Grondwet een lex specialis is van artikel 10 Grondwet (p. 31). DNB meent hieruit op te kunnen maken dat onder de reikwijdte van artikel 13 Grondwet niet de zakelijke gegevens en bescheiden vallen als bedoeld in artikel 5:17 van de Algemene wet bestuursrecht (Awb). Op grond van dat artikel is een toezichthouder bevoegd inzage te vorderen van zakelijke gegevens en bescheiden en daarvan kopieën te maken.

De vraag is of deze aanname juist is. Anderzijds is namelijk in de MvT vermeld dat het brief- en telecommunicatiebelang ziet op de bescherming van het belang dat een burger heeft bij "privé-communicatie (of vertrouwelijke communicatie)" (p. 9 MvT). Daarbij gaat het volgens de toelichting op dezelfde pagina om "communicatie die niet voor het publiek toegankelijk is, anders dan door de verzender aangewezen" en niet-openbare communicatie". Dit impliceert dat artikel 13 Grondwet zou komen te zien op alle niet-openbare communicatie, waaronder alle zakelijke gegevens en bescheiden die niet openbaar gemaakt zijn.

Indien niet wordt beoogd zakelijke berichten als bedoeld in artikel 5:17 Awb onder het brief- en telecommunicatiegeheim te laten vallen, zullen de gevolgen voor de werkwijze van DNB waarschijnlijk beperkt zijn. De als toezichthouder in de zin van de Awb aangewezen medewerkers van DNB kunnen ook thans slechts inzage vorderen in *zakelijke* gegevens en bescheiden.

Hierbij plaats DNB nog wel de volgende kanttekening. In haar toezichtonderzoeken kan DNB stuiten op een verzameling correspondentie die én zakelijk én persoonlijk van aard kan zijn, en waarvan zonder inzage in de verschillende berichten niet op voorhand beoordeeld kan worden welke berichten persoonlijk van aard zijn en welke zakelijk (denk aan e-mailboxen). Als het de bedoeling zou zijn dat toezichthouders in een dergelijk geval eerst een machtiging van de rechter verkrijgen om die beoordeling te kunnen doen, zal dat er toe leiden dat DNB die last zal moeten verkrijgen in bijna alle gevallen dat een inbox van (een medewerker van) een onderneming wordt ingezien. Dit zal naar de opvatting van DNB het toezichtproces onevenredig zwaar belasten.

De Nederlandsche Bank

De Minister van Binnenlandse Zaken en Koninkrijksrelaties

Postbus 20011
2500 EA DEN HAAG

Mocht het bovendien toch zo zijn – in afwijking van bovengenoemde aanname - dat met het wetsvoorstel is bedoeld om zakelijke gegevens en bescheiden óók onder de reikwijdte van het brief- en telecommunicatiegeheim te laten vallen, dan zullen de gevolgen daarvan voor DNB – en naar verwachting voor alle toezichthouders - aanzienlijk zijn. DNB zal dan bij elke vordering tot inzage van zakelijke gegevens en bescheiden om een machtiging van de rechter moeten verzoeken. Dit zou een beperking van deze toezichtbevoegdheid uit de Awb betekenen.

Gezien de hierboven geschetste onduidelijkheid geeft DNB u graag in overweging om in de Memorie van Toelichting enige overwegingen aan artikel 5:17 van de Awb te wijden. Uit die toelichting zou bij voorkeur van DNB opgemaakt kunnen worden dat zakelijke gegevens en bescheiden niet onder de reikwijdte van het brief- en telecommunicatiegeheim vallen.

Nationale veiligheid
De hoofdregel zal zijn dat voor beperkingen op het brief- en telecommunicatiegeheim een machtiging van de rechter vereist is. Uw eerste vraag ziet op een uitzondering op deze hoofdregel indien het belang van de nationale veiligheid aan de orde is. DNB verwacht zelden een beroep te zullen doen op een dergelijke uitzondering. De uitzondering zal daarom geen gevolgen hebben voor de werkwijze van DNB.

Regelingsopdracht
Uw tweede vraag is of DNB een meerwaarde ziet in de regelingsopdracht die volgt uit het voorgestelde artikel 13, derde lid, van Grondwet. U vroeg in het bijzonder naar een meerwaarde ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid. Uit de MvT volgt dat dit met name van belang is voor de horizontale werking van het brief- en telecommunicatiegeheim. DNB houdt geen toezicht op de naleving van regels ten aanzien van het behandelen van communicatie of andere privacy gerelateerde regels. DNB ziet daarom vanuit haar specifieke taken geen toegevoegde waarde van bedoelde regelingsopdracht.

Hoogachtend,
De Nederlandsche Bank NV

Drs. G.J. Duitman
Afdelingshoofd

Kopie: Autoriteit Financiële Markten

COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN Minister van Binnenlandse Zaken en Koninkrijkrelaties
De heer dr. R.H.A. Plasterk
Postbus 20011
2500 EA DEN HAAG

DATUM 11 februari 2013
ONS KENMERK z2012-00746
CONTACTPERSONEN

UW BRIEF VAN 17 oktober 2012
UW KENMERK 2012-0000581107

ONDERWERP Wetgevingsadvies conceptwetsvoorstel tot wijziging van artikel 13 Grondwet

Geachte heer Plasterk,

Bij brief van 16 oktober 2012 heeft u het College bescherming persoonsgegevens (CBP) in de gelegenheid gesteld te reageren op het *conceptwetsvoorstel tot wijziging van artikel 13 Grondwet* (wetsvoorstel) in het kader van een algemene internetconsultatie. Voor de goede orde verwijst het CBP naar zijn eerdere brief van 6 december 2012 inzake zijn procedure om te komen tot een wetgevingsadvies conform artikel 51 lid 2 van de Wet bescherming persoonsgegevens (Wbp).

Het huidige artikel 13 van de Grondwet (het brief-, telefoon-, telegraafgeheim) zal worden aangepast aan de condities van de huidige tijd. Voor één element heeft u het CBP in het bijzonder aandacht gevraagd. Het betreft het voorgestelde derde lid van artikel 13 van de Grondwet. "*De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim.*" U heeft om de opvatting van het CBP verzocht over de vraag of een dergelijke regelingsopdracht aan de wetgever meerwaarde heeft ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid.

Hiermee voldoe ik aan uw verzoek.

Hoofdpunten van het wetgevingsadvies
Hieronder volgen de hoofdpunten van het wetgevingsadvies.

- Meerwaarde regelingsopdracht: het CBP ziet in een regelingsopdracht op grondwettelijk niveau zoals geformuleerd in het voorgestelde artikel 13, derde lid meerwaarde ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid. Desalniettemin plaatst het CBP kanttekeningen bij deze regelingsopdracht.

- Verkeersgegevens: het valt niet zonder meer in te zien waarom in het voorgestelde artikel 13 van de Grondwet ten aanzien van het beschermingsniveau onderscheid zou dienen te worden gemaakt tussen verkeersgegevens en de communicatie-inhoud, mede in het licht van het

DATUM 11 februari 2013
ONS KENMERK z2012-00746

bepaalde in artikel 8 van het EVRM en artikel 7 van het Handvest van de grondrechten van de Europese Unie (Handvest).

- Informed consent: het CBP adviseert de passages over 'informed consent' in de MvT bij het voorgestelde artikel 13 van de Grondwet zodanig aan te passen dat de voorwaarden voor een geldige toestemming volledig hun weerslag krijgen in de MvT.

- Beperkingen: het CBP merkt op dat de MvT ruimte laat voor de mogelijkheid dat de burger mogelijkerwijs minder bescherming zou kunnen ontlenen aan het voorgestelde artikel 13 van de Grondwet dan aan artikel 8 van het EVRM, door het verschil in de aard van de gestelde beperkingseisen. Deze keuze is onvoldoende gemotiveerd.

- Integriteit persoonsgegevens opgeslagen in randapparatuur: een laatste, maar niet minder belangrijk punt, betreft de noodzaak tot grondwettelijke bescherming van gegevens opgeslagen in randapparatuur. In het licht van het bepaalde in artikel 8 van het EVRM en artikel 7 van het Handvest zou het voorgestelde artikel 13 van de Grondwet ten aanzien van het beschermingsniveau geen onderscheid moeten maken tussen gegevens opgeslagen in randapparatuur en opgeslagen bij een derde.

Conclusie
Het CBP is van oordeel dat het wetsvoorstel op de punten genoemd in het wetgevingsadvies aanpassing en/of nadere motivering behoeft. Het CBP heeft bezwaar tegen het voorstel (van wet) en adviseert u dit niet aldus in te dienen.

Voor het volledige advies verwijs ik u naar de bijlage bij deze brief. Voor een nadere toelichting op het advies ben ik graag beschikbaar.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

Het advies van het College bescherming persoonsgegevens van 11 februari 2013 over het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet (z2012-00746)

Inleiding

Bij brief van 16 oktober 2012 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) het College bescherming persoonsgegevens (CBP) in de gelegenheid gesteld te reageren op het *conceptwetsvoorstel tot wijziging van artikel 13 Grondwet* (wetsvoorstel) in het kader van een algemene internetconsultatie. Het huidige artikel 13 van de Grondwet (het brief-, telefoon-, telegraafgeheim) zal worden aangepast aan de condities van de huidige tijd. Voor één element vraagt de minister het CBP in het bijzonder aandacht. Het betreft het voorgestelde derde lid van artikel 13 van de Grondwet. "*De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim.*" De minister vraagt de opvatting van het CBP of een dergelijke regelingsopdracht aan de wetgever meerwaarde heeft ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid.

De reacties van het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA)[1] en het College voor de Rechten van de Mens[2] op het wetsvoorstel zijn in dit advies betrokken.

Achtergrond

Dit wetsvoorstel strekt ertoe de reikwijdte van de onschendbaarheid van het brief-, telefoon-, en telegraafgeheim dat in artikel 13 van de Grondwet is neergelegd uit te breiden naar alle communicatiemiddelen. In de praktijk voldoet volgens de memorie van toelichting (MvT) de huidige grondwettelijke bepaling niet langer; de modernisering van artikel 13 van de Grondwet zal moeten leiden tot een techniekonafhankelijke benadering van de reikwijdte. De directe aanleiding voor onderhavig wetsvoorstel is gelegen in het rapport van de Staatscommissie Grondwet van november 2010 en de daaropvolgende kabinetsreactie. Het kabinet oordeelde in reactie op het advies van de Staatscommissie Grondwet dat de techniekonafhankelijke en limitatieve formulering van de beschermde communicatiemiddelen de normatieve betekenis van artikel 13 aan de wetgever en rechter in de weg staat. Zij leidt tot netelige interpretatievraagstukken en het risico van inconsistentie in de uitleg en de beoogde en gewenste rechtsbescherming. Dit probleem wordt versterkt doordat de formulering van artikel 13 van de Grondwet ver achter loopt bij de verwante verdragsrechten waarin de laatste jaren nieuwe ontwikkelingen, normen en formuleringen zijn uitgekristalliseerd.

Inhoud wetsvoorstel

De Minister van BZK vraagt het CBP om advies over het voorgestelde artikel 13 van de Grondwet.

---

[1] Advies van 19 december 2012 van het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) op het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet, URL: http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3703.

[2] Advies van 15 januari 2013 van het College van de Rechten van de Mens op conceptwetsvoorstel tot wijziging van artikel 13 Grondwet, URL: http://www.mensenrechten.nl/publicaties/detail/17789.

Artikel 13 Grondwet (voorstel) luidt:

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

Het wetsvoorstel strekt tot modernisering van het huidige artikel; met dit wetsvoorstel wordt volgens de MvT gestreefd naar een volledige techniekonafhankelijke bescherming. Het brief-, telefoon-, en telegraafgeheim zoals vastgelegd in het huidige artikel 13 van de Grondwet beschermt tegen inzage in de communicatie van staatswege. Normgeadresseerde is aldus de drager van publiek gezag of staatsmacht. Het brief- en telecommunicatiegeheim, dat het huidige artikel 13 Grondwetsartikel zal gaan vervangen, richt zich dus primair tegen (heimelijke) inzage in de inhoud van communicatie door de overheid.

Het brief- en telecommunicatiegeheim ziet op de bescherming van het belang dat de burger heeft bij privé-communicatie (of vertrouwelijke communicatie). Met privé-communicatie wordt blijkens de MvT bedoeld communicatie die niet voor het publiek toegankelijk is, anders dan door de verzender aangewezen. Het gaat aldus om niet-openbare communicatie. Openbare communicatie wordt beschermd door het recht op vrijheid van meningsuiting (artikel 7 van de Grondwet). Veelal wordt privé-communicatie gezien als één specifiek aspect van de persoonlijke levenssfeer dat bijzondere bescherming toekomt. De persoonlijke levenssfeer wordt beschermd door artikel 10 van de Grondwet.

Reikwijdte

Om te kunnen bepalen of het brief- en telecommunicatiegeheim in een concrete situatie aan de orde is, worden in de MvT drie cumulatieve criteria gehanteerd:

- het gebruik van een communicatiemiddel in het communicatieproces: wat 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.
- de aanwezigheid van een derde die belast is met het beheer over de overdracht en/of opslag van de communicatie: de technologische werkelijkheid, waarin opslag en overdracht van het bericht als het ware met elkaar versmelten dient te worden vertaald in de reikwijdte van het brief- en telecommunicatiegeheim omdat de bescherming heeft te gelden zolang de derde feitelijk toegang tot de inhoud van het bericht heeft.
- de noodzaak van de 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.

Beoordeling

In zijn algemene en specifieke beoordeling richt het CBP zich op de gevolgen van het wetsvoorstel voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer van de burger, waarbij in het bijzonder aandacht wordt besteed aan de concrete vraag van de minister over de meerwaarde van de regelingsopdracht aan de wetgever ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid.

Algemene beoordeling

Het CBP is, net als het College voor de Rechten van de Mens en OPTA, van oordeel dat de modernisering in de vorm van een techniekonafhankelijke invulling van artikel 13 van de Grondwet een bij de huidige tijd passende wijziging is. Het brief- en telecommunicatiegeheim verdient eenzelfde bescherming in een digitale als in een niet-digitale omgeving. Door deze wijziging zal in beginsel de verwerking van persoonsgegevens via huidige en toekomstige communicatiemiddelen een passende bescherming kunnen verkrijgen, indien rekening wordt gehouden met het advies van het CBP.

Verder is het CBP in algemene zin van oordeel dat een regelingsopdracht zoals geformuleerd in het voorgestelde artikel 13, derde lid, van de Grondwet van meerwaarde is ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid. Het CBP heeft desondanks een aantal kritische aandachtspunten ten aanzien van deze delegatiebepaling die onder het kopje "Meerwaarde regelingsopdracht" aan bod zullen komen.

Het CBP constateert voorts met instemming dat de bescherming van het voorgestelde artikel 13 van de Grondwet niet beperkt blijft tot de zogenoemde 'transportfase', maar dat het voorziet in bescherming voor zover en zolang de inhoud van communicatie aan een derde voor de overdracht en/of opslag is toevertrouwd, behoudens het opgemerkte onder het kopje "Elektronische communicatienetwerken en –diensten". Dit (mede) gelet op de technologische werkelijkheid, waarin opslag en overdracht van communicatie als het ware met elkaar versmelten.

Specifieke beoordeling

Hieronder zal het CBP ingaan op een aantal specifieke punten.

1. Meerwaarde regelingsopdracht

In de MvT (p. 14) staat vermeld dat in het leeuwendeel van de gevallen het niet de overheid is als derde die de overdracht en eventueel opslag van de vertrouwelijke communicatie verzorgt, maar een private partij. *"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 zelfs nooit in handen geweest van de overheid"*, (MvT, p. 18). Het brief-, telefoon-, en telegraafgeheim zoals vastgelegd in het huidige artikel 13 van de Grondwet beschermt tegen inzage in de communicatie van staatswege (MvT, p. 9). Volgens de MvT (p. 18) kan een bepaling inzake de horizontale werking van het voorgestelde artikel 13, gelet op de systematiek van hoofdstuk 1 van de

Grondwet, enkel worden geformuleerd in de vorm van een regelingsopdracht aan de formele wetgever.

Grondrechten hebben naar hun oorspronkelijke bedoeling uitsluitend verticale werking en zijn historisch gezien gericht op de gezagsrelatie tussen overheid en burger. In de huidige tijd is echter wel een in kracht en betekenis toenemende tendens ontstaan om de gelding van grondrechten ook uit te doen strekken over rechtsbetrekkingen tussen burgers en tussen burgers en particuliere organisaties.[3] Zo kan (naar analogie) uit de in 2010 door het ministerie van Justitie afgegeven Leidraad afstemmen wetgeving op de Wet bescherming persoonsgegevens worden afgeleid (p. 26): *"Zowel artikel 8 EVRM als artikel 10 van de Grondwet heeft horizontale werking en normeert daarom niet alleen de verhouding tussen de overheid en de burger maar werkt ook door in de rechtsbetrekkingen tussen burgers onderling."*[4]

In de MvT (p. 35) staat vermeld dat de huidige Tw zich goed verhoudt tot het voorstel voor het nieuwe artikel 13 en dat deze reeds uitvoering geeft aan de regelingsopdracht in het derde lid van het wetsvoorstel. Voor wat betreft de openbare elektronische communicatienetwerken en -diensten vult de Tw een groot deel van de lacunes in de bescherming van het brief- en telecommunicatiegeheim in horizontale verhoudingen, aldus de MvT (p. 35). In de MvT (p. 33) wordt aangehaald dat: *"Art. 18.13 lid 1 Tw (...) een instructie van de wetgever aan de lagere wetgever en de uitvoerende instanties* [bevat, toevoeging door het CBP] *om bij het nemen van maatregelen en het stellen van regels bij of krachtens de Tw het belang van de bescherming van de persoonsgegevens en de bescherming van de persoonlijke levenssfeer alsmede de bescherming van het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken in acht te nemen. Het tweede lid van art. 18.13 Tw verklaart het eerste lid van overeenkomstige toepassing op de bedrijfsvoering door aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten. Aanbieders mogen aldus op grond van dit tweede lid geen kennis nemen van de inhoud van de communicatie of verkeersgegevens verwerken, tenzij dat uitdrukkelijk bij of krachtens de Tw is toegestaan."*

Het CBP onderschrijft dat de in de MvT (p. 33-35) aangehaalde bepalingen uit de Tw (al) een groot deel van de lacunes invullen van de bescherming van het brief- en telecommunicatiegeheim in horizontale relaties bij openbare elektronische communicatienetwerken en -diensten. Hoewel het brief- en telecommunicatiegeheim zich primair richt tegen heimelijke inzage in de inhoud door de overheid en het in de regel niet de overheid is die de overdracht en eventueel opslag van de vertrouwelijke communicatie verzorgt, maar een private partij ziet het CBP in een regelingsopdracht *op grondwetsniveau* zoals geformuleerd in het voorgestelde artikel 13, derde lid toch meerwaarde ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid. Ook het College voor de Rechten van de Mens signaleert in zijn advies (p. 9) inzake het thans voorliggende wetsvoorstel dat met de toegenomen rol van private partijen in (tele-) communicatiesystemen, het belang van de bescherming van het communicatiegeheim in horizontale verhoudingen steeds groter wordt.

---

[3] Zie: o.a. M.C. Burkens e.a, *Beginselen van de democratische rechtsstaat. Inleiding tot de grondslagen van het Nederlandse staats- en bestuursrecht*, Deventer: W.E.J. Tjeenk Willink 2006, p. 140. Vgl. ook Van der Pot-Donner, *Handboek Van Het Nederlandse Staatsrecht*, Deventer: Kluwer 2006, p. 284 e.v.; C.A.J.M. Kortmann, *Constitutioneel recht*, Deventer: Kluwer 2008, p. 387.

[4] URL: https://zoek.officielebekendmakingen.nl/blg-115090.html.

Evenzeer sluit het CBP zich aan bij het advies van OPTA op het wetsvoorstel (p. 3), te weten dat het aannemelijk is dat het stelsel van hoofdstuk 11 en artikel 18.13 van de Tw verdere herformulering en/of invulling behoeft om aan de strekking van het voorgestelde artikel 13 van de Grondwet invulling te geven en het bijbehorende verzoek om waar nodig de terminologie en formulering daarvan nader te bezien (in samenhang met deze grondwetswijziging).

2. Verkeersgegevens

In de MvT (p. 12, 16-18) wordt aangegeven dat verkeersgegevens, voor zover ze tevens persoonsgegevens zijn, op dit moment worden beschermd door artikel 10 van de Grondwet (recht op eerbiediging van de persoonlijke levenssfeer). Deze gegevens behoren volgens de MvT niet primair tot het belang dat artikel 13 van de Grondwet beoogt te beschermen, omdat zij niet de inhoud van het bericht weergeven. Niet kan worden uitgesloten dat zij daarvan wel deel uitmaken indien zij nauw verband houden met de inhoud van het bericht.[5]

In de MvT (p. 17) staat verder vermeld: *"Verkeersgegevens geven op zich geen inzicht in de inhoud van de communicatie, maar wel in andere aspecten die verband kunnen houden met de inhoud van de communicatie. Verkeersgegevens kunnen bovendien naar hun aard raken aan de telecommunicatievrijheid."* Anders gezegd, zou een gebruiker weten of vermoeden dat de overheid weet welke communicatie hij voert, dan doorbreekt dat de vertrouwelijkheid van de communicatie op zichzelf niet, maar kan het voor hem wel reden zijn om bepaalde communicatie niet meer te voeren.

Het CBP wijst erop dat zowel de inhoud van, als 'informatie over elektronische communicatie' (oftewel, verkeersgegevens) gegevens zijn die bescherming genieten op grond van artikel 8 van het EVRM en artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie (Handvest)[6]. Het Europees Hof voor de Rechten van de Mens (EHRM) oordeelde in zijn arrest van 3 april 2007 over de bescherming van e-mailcorrespondentie en internetgebruik: *"Accordingly, the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8"*, (onderstreping toegevoegd door het CBP).[7] Zie in dezelfde zin het arrest van het EHRM van 2 augustus 1984 over de bescherming van verkeersgegevens: *"By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. 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*

---

[5] *Kamerstukken II* 2000/01, 27 460, nr. 2, p. 61. In het kabinetsstandpunt over het rapport van de Commissie Grondrechten in het digitale tijdperk is hierover opgemerkt: *"Voor zover kennisneming van verkeersgegevens samenvalt met kennisneming van gegevens over de inhoud, is er overigens tevens sprake van inhoudsgegevens." Kamerstukken II* 2000/01, 27 460, nr. 1, p. 27.

[6] De in artikel 7 van het Handvest gewaarborgde rechten corresponderen met de rechten die in artikel 8 van het EVRM zijn gewaarborgd. Dit recht heeft dezelfde inhoud en reikwijdte als het recht in de daarmee corresponderende bepaling van het EVRM. Artikel 8 van het Handvest is een afzonderlijke bepaling over de bescherming van persoonsgegevens. Toelichtingen bij het Handvest van de grondrechten. URL: http://eur-lex.europa.eu/nl/treaties/dat/32007X1214/htm/C2007303NL.01001701.htm.

[7] EHRM 3 april 2007, *NJ* 2007, 617 (Copland/Verenigd Koninkrijk), r.o. 44.

under Art. 8. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone", (onderstreping toegevoegd door het CBP).[8] Ook in de MvT aangehaalde Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society van 13 maart 2005 wordt als vaststaand beschouwd dat zowel de inhoud van communicatie als verkeersgegevens bescherming genieten op grond van artikel 8 van het EVRM: *"Any use of ICTs should respect the right to private life and private correspondence. (...) Both the content and traffic data of electronic communications fall under the scope of Article 8 of the ECHR and should not be submitted to restrictions other than those provided for in that provision. (...)."*[9]

Het CBP begrijpt verder uit de MvT (p. 10-11) dat de gebezigde term "telecommunicatie" ruimer zal moeten worden geïnterpreteerd dan in de Tw, de Europese richtlijnen of in het Verdrag van de Internationale Unie voor Telecommunicatie. De term ziet op alle huidige en toekomstige communicatiemiddelen en niet alleen op elektronische communicatie.

Nu (i) verkeersgegevens als 'een integraal onderdeel van de communicatie' bescherming genieten onder artikel 8 van het EVRM dat onder andere de "correspondentie" beschermt, (ii) dit artikel 8 van het EVRM sterke gelijkenis vertoont met artikel 7 van het Handvest, met dien verstande dat het woord "correspondentie" is vervangen door "communicatie" en (iii) de term "telecommunicatie" in het voorgestelde artikel 13 van de Grondwet ruim dient te worden uitgelegd - ruimer dan de term "elektronische communicatie", valt niet zonder meer in te zien waarom in het voorgestelde artikel 13 van de Grondwet qua bescherming onderscheid zou dienen te worden gemaakt tussen verkeersgegevens en de communicatie-inhoud.[10]

Subsidiair wijst het CBP op het volgende. De begripsafbakening tussen "inhoud van de communicatie" en "verkeersgegevens" wordt bemoeilijkt door de steeds sterkere vervlechting van de gevoerde communicatie en de daarmee samenhangende gegevens in de technische protocollen. Bij spraaktelefonie kan het onderscheid tussen deze begrippen nog worden gemaakt langs de lijn van de technische scheiding tussen spraak- (dat wat wordt gezegd) en signaleringskanaal (dat wat nodig is om de verbinding tot stand te brengen). Bij communicatietoepassingen zoals mobiele telefonie en internet is dat niet langer zonder meer het geval (het http protocol bevat zowel inhoudskenmerken als verkeersgegevens: de URL heeft in de meeste gevallen ook een inhoudelijke waarde, in die zin dat daaruit informatie is af te lezen over de communicatie-inhoud). Het CBP sluit daarbij ook aan bij hetgeen het College van de Rechten voor de Mens hierover in zijn advies (p. 8) schrijft: *"Uit de literatuur beschreven praktijk over het heimelijk onderscheppen van communicatiegegevens door veiligheidsdiensten komt het beeld naar voren dat het op voorhand niet altijd duidelijk is of de grote hoeveelheid gegevens die op deze wijze wordt 'binnengehaald' alleen bestaat uit verkeersgegevens of ook uit gegevens met betrekking tot de inhoud van de communicatie. Het vasthouden aan een dergelijk onderscheid lijkt dan ook te duiden op een logisch tekort: dat sprake is van inhoudsgegevens kan pas blijken nadat de gegevens reeds zijn binnengehaald onder het regime dat geldt voor verkeersgegevens."*

[8] EHRM 2 augustus 1984, *NJ* 1988, 534 (Malone/Verenigd Koninkrijk). Zie ook EHRM 25 september 2001, *NJ* 2003, 670 (P.G. en J.H./Verenigd Koninkrijk).
[9] Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society van 13 maart 2005, CM(2005)56.
[10] Vgl. ook overweging 21 bij en artikel 5 van de e-Privacyrichtlijn.

Omdat verkeersgegevens veel over de gebruiker kunnen zeggen en raken aan de telecommunicatievrijheid, worden verkeersgegevens die ook persoonsgegevens zijn ook wel aangeduid als gegevens van gevoelige aard. In (de antwoorden op de vragen over) het kabinetsstandpunt over het rapport van de Commissie Grondrechten in het digitale tijdperk is hierover opgemerkt: *"Verkeersgegevens kunnen veel over personen zeggen. Dit geldt echter voor meer soorten van gevoelige gegevens."*[11]

Gelet op het voorgaande dient volgens het CBP nadere aandacht te worden geschonken aan de reikwijdte van het voorgestelde artikel 13 van de Grondwet (de uitzondering voor verkeersgegevens, zie MvT, p. 16-18). Subsidiair adviseert het CBP de desbetreffende passages in de memorie van toelichting bij artikel 13 van de Grondwet op het punt van het afbakeningsprobleem tussen verkeersgegevens en inhoud van de communicatie te verduidelijken en aan te vullen.

Het CBP sluit zich voor het overige aan bij de reactie van OPTA op het wetsvoorstel (p. 4) met het advies nadere aandacht te geven aan het afbakeningsprobleem tussen verkeersgegevens en inhoud van de communicatie bij de uitwerking van het brief- en telecommunicatiegeheim in de (lagere) wet- en regelgeving.

3. Samenloop Wbp en Tw

In de MvT (p. 28) staat vermeld: *"Naast het algemene kader van de Privacyrichtlijn werd een specifiek op de telecommunicatiesector toegesneden regeling noodzakelijk geacht. De ePrivacyrichtlijn, een lex specialis van de Privacyrichtlijn, beschermt de persoonlijke levenssfeer van gebruikers van openbare elektronische communicatienetwerken en -diensten."*

Het CBP wijst erop dat de e-Privacyrichtlijn (geïmplementeerd in de Telecommunicatiewet; Tw) zich verhoudt tot de Privacyrichtlijn (geïmplementeerd in de Wbp) als sectorale tot algemene regels. Op dezelfde manier is de verhouding tussen de Tw en de Wbp er volgens het CBP in algemene zin een van (aanvullende) sectorale normen naast - en niet in plaats van - de Wbp. Er is in algemene zin geen sprake van een lex specialis-situatie: een bijzondere wet die altijd voorrang krijgt boven een algemene. Wel geldt dat indien en voor zover de e-Privacyrichtlijn (geïmplementeerd in de Tw) ten aanzien van de verwerking van persoonsgegevens op een bepaald punt een uitputtende regeling bevat, die regeling voorgaat op de algemene normen uit de Privacyrichtlijn (geïmplementeerd in de Wbp).[12]

Uit de tekst van artikel 3, eerste lid, van de Privacyrichtlijn volgt dat deze een algemeen - niet sectoraal - toepassingsbereik heeft. De algemene Privacyrichtlijn is daarom mede van toepassing op de verwerking van persoonsgegevens in de telecommunicatiesector.[13] Uit de tekst van artikel 1, tweede lid, van de telecomspecifieke e-Privacyrichtlijn volgt dat de bepalingen van deze richtlijn 'een specificatie van en een aanvulling' vormen op de Privacyrichtlijn.[14]

---

[11] Zie ook idem, nr. 1, p. 27: *"(...) het feit dat verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen, maar dat datzelfde geldt voor veel meer gevoelige gegevens (...)."*
[12] Zie ook: *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 45.
[13] Zie ook: *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 13.
[14] Zie ook overweging 10 van de e-Privacyrichtlijn: *"In de sector elektronische communicatie is Richtlijn 95/46/EG van toepassing, met name op alle aangelegenheden met betrekking tot de bescherming van fundamentele rechten en vrijheden die niet specifiek onder het bepaalde in deze richtlijn vallen, met inbegrip*

Beide richtlijnen zijn in de telecommunicatiesector cumulatief van toepassing. De richtlijnen hebben (deels) een ander karakter[15] en een ander toepassingsbereik. Dat wil zeggen dat - anders dan de Privacyrichtlijn - de e-Privacyrichtlijn ook van toepassing is op de verwerking van verkeersgegevens die geen persoonsgegevens zijn (de regels gelden bijvoorbeeld ook ten aanzien van gegevens van rechtspersonen). Anders dan de e-Privacyrichtlijn, geldt de Privacyrichtlijn ook voor zover het gaat om de verwerking van verkeersgegevens die ook persoonsgegevens zijn in niet-openbare (besloten) elektronische communicatienetwerken en -diensten. De bepalingen uit de e-Privacyrichtlijn geven weliswaar aan bepaalde algemene normen uit de Privacyrichtlijn een nadere invulling (bijvoorbeeld een nadere begrenzing/inperking van de toegestane verwerkingen), maar hebben ook een aanvullend karakter.[16]

Hetzelfde volgt - ten aanzien van de verhouding tussen de Wbp en de Tw - ook met zoveel woorden uit de wetsgeschiedenis bij de Wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens: *"In zijn algemeenheid kan niet worden gesteld dat bijzondere wetgeving voor de meer algemene privacyvoorschriften gaat. Dit adagium* [te weten: de regel 'lex specialis derogat legi generali'; toevoeging door het CBP] *gaat alleen op in die gevallen dat de bijzondere wet ten opzichte van de Wbp een exclusieve werking heeft, dat wil zeggen een uitputtende regeling bevat waarnaast de Wbp geen gelding meer heeft. Een opsomming van dergelijke specifieke wetgeving staat in artikel 2 van de Wbp. In de gevallen dat de specifieke wetgeving niet valt onder het bereik van dit artikel 2, geldt de regel «bijzondere wet gaat voor algemene wet» echter niet. De Wbp geldt in deze gevallen immers naast de specifieke wetgeving. Alsdan heeft de Wbp dus een aanvullende werking, namelijk voor die onderdelen die niet door de bijzondere wetgeving worden gedekt. De Organisatiewet sociale verzekeringen 1997 en de Telecommunicatiewet zijn daar een voorbeeld van. De geheimhoudingsvoorschriften in de Organisatiewet sociale verzekeringen vormen dus een uitwerking van die in de Wbp. Wel is het zo dat de voorschriften van de Wbp daarmee niet als direct bindende normen in beeld komen, ze spelen enkel zijdelings een rol."*[17]

Gelet op het voorgaande adviseert het CBP de desbetreffende passage in de memorie van toelichting bij het voorgestelde artikel 13 van de Grondwet met deze beschrijving van de verhouding tussen de betreffende wetten te verduidelijken en aan te vullen.

---

van de plichten van de verantwoordelijke en de rechten van personen. Richtlijn 95/46/EG is van toepassing op niet-openbare communicatiediensten", (onderstreping toegevoegd door het CBP). Zie in dezelfde zin overweging 12, 20 en 46 en artikel 4, eerste lid bis, van de e-Privacyrichtlijn.

[15] Bijvoorbeeld: de bepalingen in de e-Privacyrichtlijn die betrekking hebben op de beschikbaarheid van nummeridentificatie. Vgl. *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 54.

[16] Zie: *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 53. Vgl. ook *Kamerstukken II* 1998/99, 25 892, nr. 6, p. 11; *Kamerstukken I* 1997/98, 25 533, nr. 309d, p. 8-9; *Kamerstukken II* 1997/98, 25 533, nr. 5, p. 115.

[17] *Kamerstukken II* 1999/2000, 26 410, nr. 7, p. 2. Zie in dat verband ook *Kamerstukken II* 2002/03, 28 851, nr. 7, p. 78-79: *"Zoals ik op eerdere vragen heb geantwoord, geldt met betrekking tot de verwerking van persoonsgegevens in de sector elektronische communicatie dat daarop in algemene zin de Wet bescherming persoonsgegevens van toepassing is; hoofdstuk 11 van de wet – dat strekt ter implementatie van richtlijn 2002/58/EG - heeft een aanvullend karakter. De toepasselijkheid van de Wet bescherming persoonsgegevens – en daarmee ook van het daarin opgenomen begrippenkader - blijkt bovendien nadrukkelijk uit artikel 11.2 van de wet, waarin wordt gesteld dat onverminderd het bepaalde in de Wet bescherming persoonsgegevens de aanbieders van openbare elektronische communicatienetwerken en -diensten een zorgplicht hebben voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van gebruikers en abonnees."*

4. Informed consent

In de MvT (p. 10) wordt aangehaald dat in horizontale relaties *"het geïnformeerd beslissen, ofwel 'informed consent'"* speelt bij bijvoorbeeld de keuze voor het gebruik van bepaalde communicatiemiddelen, netwerken en diensten. De MvT voegt daaraan toe: *"Ook dienen de Wet bescherming persoonsgegevens (Wbp) en het contractenrecht in dit verband te worden vermeld."* In de MvT (p. 26) staat verder vermeld: *"(...) Vaak zal instemming van de gebruiker over het inzien van de communicatie geschieden door aanvaarding van de algemene voorwaarden van een bedrijf (informed consent)".*

Uit deze zinsneden zou kunnen worden begrepen dat een betrokkene die een contractuele relatie aangaat met een aanbieder van een openbaar elektronische communicatienetwerk of -dienst of een dienst van de informatiemaatschappij (bijvoorbeeld een app-aanbieder), en de algemene voorwaarden van de betreffende partij accepteert, toestemming zou verlenen voor de verwerking van de hem betreffende gegevens.

Het CBP merkt op dat in een relatie als hierboven beschreven vrijwel altijd persoonsgegevens zullen worden verwerkt waarop de Wbp (mede) van toepassing is, variërend van NAW-, abonnements- en betalingsgegevens tot verkeersgegevens en de inhoud van de communicatie.

Van toestemming in de zin van de Wbp is echter slechts sprake indien deze 'vrij', 'specifiek' en 'geïnformeerd' is (artikel 1, aanhef en onder i, van de Wbp). "Vrij" betekent dat de betrokkene in vrijheid zijn wil moet kunnen uiten, zonder economische dwang.[18] "Specifiek" betekent dat de wilsuiting betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen (geen algemeen geformuleerde machtiging).[19] "Geïnformeerd" betekent dat de betrokkene moet beschikken over de noodzakelijke inlichtingen voor een goede oordeelsvorming.[20]

Ook voor "toestemming van een gebruiker of abonnee" als gebruikt in hoofdstuk 11 van de Tw geldt dat deze 'vrij', 'specifiek' en 'geïnformeerd' dient te zijn (artikel 11.1, aanhef en onder g, van de Tw jo. artikel 1, aanhef en onder i, van de Wbp).

Voor het verwerken van persoonsgegevens is een grondslag (rechtvaardigingsgrond) vereist als opgesomd in artikel 8, aanhef en onder a tot en met f, van de Wbp. Ten aanzien van de grondslag ondubbelzinnige toestemming (artikel 8, aanhef en onder a, van de Wbp), geldt het

---

[18] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65. Zie in dezelfde zin de conclusie van de Advocaat-Generaal van het Hof van Justitie van de Europese Unie van 17 juni 2010 in zaken C-92/09 en C-93/09: *"(...) een aanzienlijke economische dwang* [zou, toevoeging door het CBP] *volgens mij kunnen volstaan om de toestemming tot een niet-vrijwillige te maken (zodat geen sprake is van 'vrije wilsuiting' in de zin van artikel 2, sub h, van richtlijn 95/46)."*

[19] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65. In de opinie van de Artikel 29 Werkgroep is daarover opgemerkt: *"Een algemene toestemming zonder dat precies is aangegeven wat het doel is van de verwerking waarmee de betrokkene instemt, voldoet niet aan dit vereiste. Dat betekent dat de informatie over het doel van de verwerking niet in de algemene voorwaarden moet worden opgenomen, maar in een aparte toestemmingsclausule."* WP29 187, Advies 15/2011 over de definitie van "toestemming" van 13 juli 2011, p. 40. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[20] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 65.

volgende. "Ondubbelzinnige toestemming" betekent dat de verantwoordelijke niet mag uitgaan van toestemming indien de betrokkene geen opmerkingen maakt over de gegevensverwerking (oftewel: bij 'toestemming' die wordt geacht voort te vloeien uit het uitblijven van actie of het stilzwijgen van de betrokkene).[21] In de wetsgeschiedenis bij de Wbp is daarover opgemerkt: *"Als voorbeeld noem ik algemene voorwaarden die van toepassing zijn op het sluiten van een overeenkomst. Indien in dergelijke voorwaarden wordt bepaald welke gegevens er voor welk doel en door wie verwerkt worden, wil dat nog niet automatisch zeggen dat betrokkene daartoe ondubbelzinnig zijn toestemming heeft gegeven, enkel omdat hij de betreffende overeenkomst heeft ondertekend."*[22]

Het CBP en zijn rechtsvoorganger de Registratiekamer hebben door de jaren heen al vele malen vastgesteld dat geen rechtsgeldige (ondubbelzinnige) toestemming kan worden verkregen via algemene voorwaarden.[23]

Gelet op het voorgaande adviseert het CBP de desbetreffende passages in de memorie van toelichting bij het voorgestelde artikel 13 van de Grondwet op dit punt aan te passen en alle vereisten voor geldige toestemming in de MvT op te nemen. Het CBP sluit zich daarbij aan bij de reactie van OPTA op het wetsvoorstel (p. 5).

5. Beperkingen

In MvT (p. 24) wordt aangehaald dat de bestaande beperkingssystematiek van de Grondwet ongemoeid wordt gelaten en dat het wetsvoorstel in zoverre geen ruimte biedt voor de introductie van een noodzakelijkheidscriterium (naast de competentieclausuleringen en procedurele voorschriften). *"Aan de rechtsbescherming van de burger doet dat intussen niet af: indien de wetgever op het brief- en telecommunicatiegeheim een beperking wenst aan te brengen, dient deze onverkort te worden getoetst aan art. 8 EVRM. In die zin vullen artikel 8 EVRM, dat direct doorwerkt in de nationale rechtsorde, en artikel 13 elkaar aan"*, aldus de MvT (p. 24).

Uit de hierboven staande passage kan worden opgemaakt dat in de MvT lijkt te worden aanvaard dat de burger mogelijkerwijs minder bescherming zou kunnen ontlenen aan het voorgestelde artikel 13 van de Grondwet dan aan artikel 8 van het EVRM (daargelaten de voorrang van het EVRM of het Unierecht), door het verschil in de aard van de gestelde beperkingseisen. Zie in dezelfde zin: *"Wij zien het verschil in de aard van de door het EVRM en de*

---

[21] Idem, p. 66 en 67. Zie ook WP29 187, Advies 15/2011 over de definitie van "toestemming" van 13 juli 2011, p. 28 en 41.

[22] *Handelingen I* 1999/2000, 34, p. 1632. Vgl. ook HvJ EU van 19 juli 2012, zaak C-112/11 (ebookers.com), r.o. 16 en HvJ EU van 9 november 2010, zaaknummers C-92/09 en C-93/09.

[23] Zie o.a. CBP Rapport van definitieve bevindingen Onderzoek naar de verwerking van persoonsgegevens door Albert Heijn B.V. in het kader van de AH Bonuskaart/het voordeelprogramma Mijn Bonus van 9 november 2012, p. 75. URL: http://www.cbpweb.nl/downloads_rapporten/rap_2012-ah-bonus-persoonsgegevens.pdf. CBP Rapport van bevindingen over de verwerking van geolocatiegegevens door TomTom N.V. van 20 december 2011, p. 24. URL: http://www.cbpweb.nl/downloads_pb/pb_20120112_tomtom-geolocatie-persoonsgegevens-definitieve-bevindingen.pdf. Bevindingen Onderzoek door het College bescherming persoonsgegevens (CBP) naar de verwerking van persoonsgegevens door Advance Concepts B.V. van 15 december 2009, p. 27 en 28. URL: http://cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf. Zie ook M.J.T. Artz, *Koning klant. Het gebruik van klantgegevens voor marketingdoeleinden.* Achtergrondstudies en Verkenningen 14, p. 16. URL: http://www.cbpweb.nl/downloads_av/av14.pdf.

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 uitgebreidere bescherming van in dit geval het brief- en telecommunicatiegeheim. Bepalend is immers het beginsel dat de verschillende stelsels cumulatief werken: datgene waaraan de burger de meeste bescherming kan ontlenen bepaalt zijn rechtspositie. De internationale verdragen zijn complementair aan het huidige en het onderhavige voorstel voor de wijziging van artikel 13", MvT (p. 30).

De keuze om ten aanzien van dit grondrecht mogelijk een lager beschermingsniveau te garanderen in de Nederlandse Grondwet dan in het EVRM of het Unierecht is volgens het CBP onvoldoende gemotiveerd.

Gelet op het voorgaande adviseert het CBP nadere aandacht te schenken aan (het hierboven genoemde verschil in) de beperkingscriteria en de desbetreffende passages in de memorie van toelichting bij het voorgestelde artikel 13 van de Grondwet op dit punt te verduidelijken en aan te vullen.

6. Integriteit persoonsgegevens opgeslagen in randapparatuur

In de MvT (p. 12-13) is uiteengezet dat in het wetsvoorstel als uitgangspunt is genomen het vereiste van 'de aanwezigheid van een door een derde beheerd communicatiemiddel'. In de MvT (p. 14) wordt in dat verband als voorbeeld gegeven dat het voorgestelde artikel 13 van de Grondwet 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. Bij het *live*-gesprek speelt heimelijkheid van de observatie en is, al naar gelang het gesprek plaatsvindt in huiselijke sfeer dan wel in de openbare ruimte, bescherming van artikel 12 en/of artikel 10 van de Grondwet aangewezen (MvT, p. 14).

In de MvT (p. 8) is daarnaast aangehaald dat de eigenheid van vraagstukken in de online wereld niet altijd één op één te transponeren is in de offline wereld. Het CBP vraagt in dit verband nadere aandacht voor de integriteit van gegevens opgeslagen in randapparatuur.[24] Dit mede in het licht van de omstandigheid dat de Nederlandse overheid (opsporingsautoriteiten) kan beschikken over software waarmee randapparatuur van burgers heimelijk op afstand, via een internetverbinding, kunnen worden doorzocht.[25] Zulks kan voor de betrokkene(n) (in, naar mag worden verwacht, nog toenemende mate) ingrijpende gevolgen hebben, gelet op de technologische en sociale werkelijkheid waarin internet en *smart mobile devices* deel uitmaken van het dagelijks leven van iedere individuele burger.

Het CBP merkt op dat integriteit van randapparatuur een in beginsel te respecteren dimensie is van artikel 8 van het EVRM.[26] Overweging 24 van de e-Privacyrichtlijn luidt in dat verband: *"Eindapparatuur van gebruikers van netwerken voor elektronische communicatie en in die apparatuur*

---

[24] En het gaat daarbij niet alleen om opgeslagen gegevens (inhoud van privé- of zakelijke communicatie), maar ook om informatie over het communicatiegedrag van de betrokkene.
[25] Zie o.a. *Aanhangsel Handelingen II* 2011/12, nr. 1374. Vgl. ook *Aanhangsel Handelingen II* 2011/12, nr. 1382.
[26] Vgl. EHRM 1 juli 2008, *NJ* 2010, 324 (Liberty/Verenigd Koninkrijk). Het EHRM heeft onder andere beginselen en eisen geformuleerd voor het via ICT-toepassingen heimelijk onderscheppen en monitoren van communicatie.

bewaarde informatie maken deel uit van de persoonlijke levenssfeer van de gebruikers die op grond van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden bescherming vereist. Zogeheten spionagesoftware, webtaps, verborgen identificatoren en andere soortgelijke programmatuur kunnen de terminal van de gebruiker zonder diens medeweten binnenkomen teneinde toegang tot informatie te krijgen, verborgen informatie op te slaan of de activiteiten van de gebruiker te traceren en kunnen ernstig inbreuk maken op de persoonlijke levenssfeer van die gebruikers. Het gebruik van die programmatuur dient alleen te worden toegestaan voor legitieme doeleinden met medeweten van de betrokken gebruikers", (onderstreping toegevoegd door het CBP).

Opmerking verdient dat het Duitse Bundesverfassungsgericht in een zaak over (technologie die het mogelijk maakt om) heimelijk op afstand computers en computernetwerken van burgers en bedrijven te doorzoeken (infiltreren), heeft geoordeeld dat het *allgemeine Persönlichkeitsrecht*, zoals neergelegd in de Duitse Grondwet, een *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* omvat.[27]

Als gevolg van de toenemende mobiliteit van randapparatuur biedt het huisrecht (artikel 12 van de Grondwet) dat zich richt op bescherming van een fysieke ruimte, de woning, niet altijd voldoende bescherming voor gegevens opgeslagen in randapparatuur. Ook artikel 10 van de Grondwet (eerbiediging van de persoonlijke levenssfeer) dat kan worden beperkt "bij of krachtens de wet", biedt in verhouding tot artikel 8 van het EVRM en het voorgestelde artikel 13 van de Grondwet die strengere beperkingscriteria kennen, een onvoldoende beschermingsniveau.

Nu (i) integriteit van randapparatuur een in beginsel te respecteren dimensie is van artikel 8 van het EVRM dat onder andere de "correspondentie" beschermt, (ii) dit artikel 8 van het EVRM sterke gelijkenis vertoont met artikel 7 van het Handvest dat onder andere de "communicatie" beschermt, (iii) de term "telecommunicatie" in het voorgestelde artikel 13 van de Grondwet ruim dient te worden uitgelegd, en (iv) de bescherming van het voorgestelde artikel 13 van de Grondwet zich bovendien reeds uitstrekt tot communicatie opgeslagen bij een derde, is volgens het CBP in de MvT onvoldoende gemotiveerd waarom in het voorgestelde artikel 13 van de Grondwet qua bescherming onderscheid zou dienen te worden gemaakt tussen gegevens opgeslagen in randapparatuur en opgeslagen bij een derde.

Gelet op het voorgaande adviseert het CBP het voorgestelde artikel 13 van de Grondwet in die zin aan te passen dat ook gegevens opgeslagen in randapparatuur onder de bescherming van dit artikel vallen. Indien de Minister daartoe niet besluit, adviseert het CBP om de gegevens opgeslagen in randapparatuur anderszins te voorzien van een beschermingsniveau vergelijkbaar met artikel 13 van de Grondwet (nieuw).

7. Elektronische communicatienetwerken en –diensten

Uit de MvT (p. 12-15) volgt verder dat het voorgestelde brief- en telecommunicatiegeheim vertrouwelijke communicatie beschermt 'voor zover en zolang de inhoud van communicatie voor de overdracht en/of opslag is toevertrouwd aan *een derde*', bijvoorbeeld aan een aanbieder van een elektronische communicatienetwerk of -dienst.

---

[27] BVerfG 27 februari 2008, 1 BvR 370/07 en 1 BvR 595/07. URL: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

Op de betekenis van de term "voor de overdracht en/of opslag toevertrouwd aan *een derde*" wordt in de MvT niet expliciet ingegaan. Het CBP vraagt in dat verband nadere aandacht voor privé-communicatie die verloopt via (organisaties met) een eigen mailserver, zoals bedrijven wel vaker in beheer hebben.

In de MvT (p. 25, 33-35) wordt verder aangehaald dat de Tw, in tegenstelling tot de Wbp, enkel geldt voor openbare elektronische communicatienetwerken en -diensten. Op de betekenis van het brief- en telecommunicatiegeheim voor elektronische communicatienetwerken en -diensten met een besloten karakter (bijvoorbeeld een intranet) wordt in de MvT niet expliciet ingegaan. Het CBP geeft in overweging te expliciteren dat de reikwijdte van het voorgestelde artikel 13 van de Grondwet zich onder andere uitstrekt tot vertrouwelijke communicatie die plaatsvindt via openbare én besloten elektronische communicatienetwerken en -diensten.

Gelet op het voorgaande adviseert het CBP de desbetreffende passages in de memorie van toelichting bij het voorgestelde artikel 13 van de Grondwet op deze punten te verduidelijken en aan te vullen.

8. Definities

Uit de MvT (p. 12, 15-16) volgt dat het voorgestelde brief- en telecommunicatiegeheim 'gerichte communicatie' beschermt, dat wil zeggen communicatie die (uitsluitend) is gericht aan een of meer specifieke ontvangers: *"Gerichte communicatie houdt in dat het bericht van de verzender wordt verstuurd aan een of meerdere afzonderlijk te bepalen geadresseerden"*, (MvT, p. 15). In de MvT (p. 15-16) worden als voorbeelden gegeven: de e-mail evenals het tegelijk aan vele mensen een e-mail of SMS-bericht versturen, het bericht dat via social media (zoals Facebook) aan een aantal ontvangers wordt verstuurd, gerichte reclame-uitingen, het oproepen van informatie uit een digitaal netwerk (een zoekmachine, Wikipedia, YouTube of een video-on-demandprogramma van een omroep) en chatten in een besloten groep. In de MvT (p. 16) wordt verder vermeld: *"Tot ongerichte communicatie horen bijvoorbeeld de toespraak, omroep en radio met realtime-uitzendingen (al dan niet via de ether of internet), het internet of een voorstelling"*, (onderstreping toegevoegd door het CBP).

Het CBP begrijpt uit de MvT (p. 16) dat individuele herleidbaarheid van de geadresseerden bepalend is voor de kwalificatie als gerichte communicatie. Het is het CBP evenwel niet geheel duidelijk wat in de MvT wordt bedoeld met de term "het internet" in de opsomming met voorbeelden van ongerichte communicatie. Enerzijds wordt (informatie op) 'het internet' in algemene bewoordingen uitgezonderd van het voorgestelde artikel 13 van de Grondwet. Anderzijds worden in de MvT specifieke voorbeelden (zoals hierboven weergegeven) aangehaald van communicatie over/verzonden via het internet die wel onder de bescherming van dit artikel vallen. Verder vraagt het CBP nadere aandacht voor de betekenis van de termen "bericht", "verzender" en "versturen", en stelt het de vraag of deze termen (nog) volstaan waar het gaat om communicatie-uitingen zoals het 'delen van informatie' via social media.

Gelet op het voorgaande adviseert het CBP de desbetreffende passages in de memorie van toelichting bij het voorgestelde artikel 13 van de Grondwet op dit punt te verduidelijken en aan te vullen.

Conclusie

Het CBP is van oordeel dat het wetsvoorstel op de punten genoemd in het wetgevingsadvies aanpassing en/of nadere motivering behoeft. Het CBP heeft bezwaar tegen het voorstel (van wet) en adviseert u dit niet aldus in te dienen.

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KvK 34 12 12 86

M
E
W https://www.bof.nl

Ministeries van Algemene Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Veiligheid en Justitie

Betreft
Consultatie wijziging artikel 13 Grondwet

Amsterdam
31 januari 2012

Geachte heer, mevrouw,

Graag reageert de Stichting Bits of Freedom op de consultatie van het concept-voorstel ter herziening van artikel 13 Grondwet (Gw). Het is hoog tijd dat deze bepaling wordt verbeterd, want de huidige tekst is achterhaald en beschermt het grondrecht op vertrouwelijke communicatie daardoor vrijwel niet.

Het voorstel is echter teleurstellend. Het biedt onvoldoende bescherming en is onduidelijk. Als de regering het voorstel niet ingrijpend verbetert dan is het beter om het huidige artikel 13 Gw in stand te laten in de wetenschap dat het een dode letter is. Ik licht dat hieronder toe en beperk me daarbij tot de meest fundamentele bezwaren.

Ten eerste heeft de regering het concept zo vormgegeven dat het niet in de weg staat aan de geplande herziening van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). De voorgenomen introductie in de Wiv van een bevoegdheid om ongericht kabelgebonden verkeer te onderscheppen is echter een onacceptabele privacy-inbreuk. De regering geeft deze plannen al bij voorbaat ruim baan door geen rechterlijke toets te eisen als de nationale veiligheid in het geding zou zijn.

Ten tweede zou het concept zo worden ingevuld dat de huidige praktijk op het gebied van de Wet bewaarplicht telecommunicatiegegegevens (de bewaarplicht) in stand kan blijven. De regering stelt immers voor om verkeersgegevens buiten de reikwijdte van artikel 13 Gw te laten. Ook de bewaarplicht is echter een onacceptabele schending van het recht op vertrouwelijke communicatie, zoals inmiddels door verschillende constitutionele rechtbanken in Europa is

bevestigd.

Dit betekent dat het op grond van het voorgestelde artikel in ieder geval twee gevallen toegestaan zou zijn om zonder rechterlijke toets de vertrouwelijke communicatie van miljoenen onverdachte Nederlanders te onderscheppen en op te slaan. Zo een voorstel miskent de kern van het grondrecht op vertrouwelijke communicatie en hoort niet in de Grondwet thuis.

Zelfs in die gevallen waar een rechterlijke toets is voorgeschreven, blijft onduidelijk wat die toets precies inhoudt. Onder het huidige voorstel is denkbaar dat een rechterlijke toets zich beperkt tot een controle of voldaan is aan formele vereisten, en dat geen onderzoek wordt gedaan naar de proportionaliteit en subsidiariteit van de inzet van een bepaald middel. Dit is des te belangrijker nu uit de toelichting blijkt dat de regering heeft gekozen om de proportionaliteitstoets van artikel 8 EVRM niet over te nemen.

Het voorstel is verder onduidelijk. Zo wordt op een cruciaal punt een veel te brede term gebruikt. In de toelichting wordt namelijk een paar keer opgemerkt dat informatie 'op het internet' ongericht - en dus onbeschermd - is (zie bijvoorbeeld pp. 15 en 16). De term 'internet' is echter heel breed: dit kan allerlei soorten communicatie omvatten, zoals communicatie via Facebook, peer-to-peer kanalen, privé-fora en apps. Uit de huidige toelichting is dus niet op te maken welke informatie wel of niet beschermd wordt door artikel 13 Gw.

Bits of Freedom concludeert dan ook dat het huidige voorstel voor artikel 13 Gw het recht op vertrouwelijke communicatie onvoldoende beschermt. Het artikel moet in ieder geval grondig worden verbeterd met inachtneming van de bovenstaande punten, wil een serieus debat over de details nuttig zijn.

Ik licht het bovenstaande graag toe, mocht daaraan behoefte bestaan.

Hoogachtend,

Ot van Daalen
Directeur Bits of Freedom

COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Minister van Binnenlandse Zaken en Koninkrijksrelaties
De heer dr. R.H.A. Plasterk
Schedeldoekshaven 200
2511 EZ Den Haag

Ons kenmerk
2012/0209

Uw kenmerk

Datum
20 december 2012

Onderwerp: Consultatie conceptvoorstel tot wijziging van artikel 13 Grondwet

Geachte heer Plasterk,

Op 1 oktober 2012 is de consultatie opengesteld betreffende het conceptvoorstel tot wijziging van artikel 13 Grondwet, het recht op brief- en telecommunicatiegeheim. De wijze waarop dit recht in de Grondwet wordt vormgegeven, is richtinggevend voor de inzet van bijzondere bevoegdheden door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). De Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (hierna: de Commissie) maakt conform haar wettelijke taak (artikel 64 lid 2 sub b van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002)) graag van de gelegenheid gebruik om u van advies te voorzien inzake het conceptvoorstel.

In de Memorie van Toelichting (MvT) van het wetsvoorstel wordt uitgelegd dat artikel 13 Grondwet de inhoud van communicatie beschermt die via een communicatiemiddel wordt verzonden. Uit de MvT wordt echter niet duidelijk of dit bescherming behelst tegen de *interceptie* van de communicatie, of enkel tegen de *selectie* of het *kennisnemen* van de communicatie. Dit onderscheid is vooral van belang voor de ongerichte interceptie in het kader van artikel 27 Wiv 2002. Bij de totstandkoming van de Wiv 2002 stelde de regering dat bij ongerichte interceptie geen sprake is van een inbreuk op artikel 13 Grondwet zolang er nog geen kennis wordt genomen van de inhoud van de gegevens.[1] Daarom was er voor de bevoegdheid tot ongerichte interceptie ingevolge artikel 27 lid 2 Wiv 2002 geen toestemming vereist als bedoeld in artikel 19 Wiv 2002. Van een inbreuk van artikel 13 Grondwet was volgens de regering pas sprake op het moment dat de gegevens geselecteerd worden. De regering merkte bij deze bevoegdheid op weinig toegevoegde waarde te zien in het stellen van een toestemmingsvereiste. Een dergelijk toestemmingsvereiste zou slechts betrekking

[1] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 44.

Anna van Saksenlaan 50 2593 HT Den Haag
T 070-3155820 F 070-3817168 www.ctivd.nl info@ctivd.nl

hebben op het satellietkanaal ten aanzien waarvan de interceptie plaatsvindt en heeft dan weinig inhoudelijke betekenis. Dit is een begrijpelijk standpunt. Maar in de voorliggende voorstel om artikel 13 Grondwet te wijzigen wordt bepleit dat het brief- en telecommunicatiegeheim betrekking heeft op de bescherming van het vertrouwelijk transport en beheer van de communicatie. Dit zou betekenen dat zodra communicatie wordt geïntercepteerd, de vertrouwelijkheid van het transport is geschonden en er dus een inbreuk van het grondwettelijk beschermde brief- en telecommunicatiegeheim heeft plaatsgevonden. De Commissie heeft deze problematiek reeds aangekaart in haar toezichtsrapport inzake de inzet van Sigint door de MIVD.[2] Gezien het belang voor de praktijk van de inzet van bijzondere bevoegdheden door de AIVD en de MIVD adviseert de Commissie om over deze kwestie helderheid te verschaffen in de MvT van het conceptvoorstel.

Als hoofdregel voor het beperken van het brief- en telecommunicatiegeheim wordt in het voorgestelde artikel 13 lid 2 Grondwet gegeven dat een rechter hiervoor toestemming moet geven. De hoofdregel wordt direct gevolgd door een uitzondering in het belang van de nationale veiligheid. Bij beperkingen van het brief- en telecommunicatiegeheim door de AIVD of de MIVD is geen toestemming van een rechter nodig, maar volstaat een machtiging van een of meer bij de wet aangewezen ministers. Deze uitzondering past in de wettelijke systematiek van de Wiv 2002.

In de MvT wordt vervolgens uitgelegd dat de minister de bevoegdheid om toestemming te geven voor een inbreuk op artikel 13 Grondwet niet mag delegeren maar wel mag mandateren (p. 22). Het verschil tussen delegatie en mandaat is dat bij delegatie degene die de bevoegdheid ontvangt, deze onder zijn eigen verantwoordelijkheid gaat uitoefenen (artikel 10:13 Awb) en bij mandaat het overdragende bestuursorgaan nog steeds verantwoordelijk blijft (artikel 10:1 Awb). De minister moet de zeggenschap houden en de verantwoordelijkheid dragen, wat volgens de MvT een reden is om delegatie niet toe te staan en mandaat wel. Waarom mandaat in dit geval noodzakelijk is, legt de MvT niet uit.

De Commissie plaatst echter haar vraagtekens bij deze algemene mogelijkheid tot mandaat. Hoewel in de MvT wordt benadrukt dat het voorstel aansluiting zoekt bij bestaande praktijk, betekent de algemene mogelijkheid van mandaat namelijk een afwijking van de Wiv 2002. Bij de totstandkoming van de Wiv 2002 is er immers voor gekozen om niet te voorzien in een mandaatregeling bij de bijzondere bevoegdheden die inbreuk maken op meer specifiek door de Grondwet geregelde rechten, waaronder het telefoon- en telegraafgeheim.[3] Dit betekent dat voor de inzet van de afluisterbevoegdheid en de selectie van Sigint op grond van de artikelen 19 j° 25 en 27 Wiv 2002 uitsluitend de verantwoordelijke minister bevoegd is om aan de AIVD en de MIVD toestemming te geven om te tappen.

Ook verhoudt de algemene mogelijkheid tot mandaat zich slecht tot de jurisprudentie van het EHRM en tot het eerder in de MvT opgenomen uitgangspunt dat toestemming moet

---

[2] Paragraaf 3.2 van het toezichtsrapport nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), beschikbaar op www.ctivd.nl.
[3] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 44.

Anna van Saksenlaan 50 2593 HT Den Haag
T 070-3155820 F 070-3817168 www.ctivd.nl info@ctivd.nl

worden gegeven door een functionaris die niet betrokken is bij het uitvoerende proces (p. 21). De Commissie adviseert de MvT op dit punt te herzien.

Hoogachtend,

Mr. A.H. van Delden
Voorzitter CTIVD

Mr. H.T. Bos-Ollermann
Secretaris CTIVD

Anna van Saksenlaan 50 2593 HT Den Haag
T 070-3155820 F 070-3817168 www.ctivd.nl info@ctivd.nl

NEDERLANDSE VERENIGING VOOR RECHTSPRAAK

De minister van Binnenlandse Zaken en Koninkrijksrelaties
Dhr. R.H.A. Plasterk
Postbus 20011
2500 EA Den Haag

Datum
1 februari 2012

Uw kenmerk
2012-0000594389

Contactpersoon

Onderwerp
Advies op wetsvoorstel tot herziening van artikel 13 Grondwet

Geachte heer Plasterk,

Bij brief van 16 oktober 2012, met kenmerk 2012-0000594389, heeft u de Nederlandse Vereniging voor Rechtspraak (hierna: NVvR) advies gevraagd over een wetsvoorstel tot wijziging van artikel 13 van de Grondwet. Dit advies is voorbereid door leden van de vereniging en is vastgesteld door de Wetenschappelijke Commissie van de NVvR.

Strekking wetsvoorstel

Het huidige artikel 13 van de Grondwet beschermt het brief-, telefoon- en telegraafgeheim. Het artikel belichaamt het recht om zonder dat derden kennis kunnen nemen van de inhoud van een bericht, gebruik te maken van de aangewezen communicatiemiddelen, aldus valt te lezen op pagina 12 van de memorie van toelichting bij dit wetsvoorstel. Het onderhavige wetsvoorstel voorziet in de uitbreiding van de reikwijdte van deze grondwetsbepaling naar alle mogelijke communicatiemiddelen.

Door het hanteren van de term "brief- en telecommunicatiegeheim" wordt dit grondrecht techniek-onafhankelijk geformuleerd. Als gevolg van elkaar snel opvolgende ontwikkelingen van de digitale mogelijkheden is het bijvoorbeeld mogelijk geworden om te communiceren via het plaatsen van persoonlijke bestanden in 'the cloud'. Nu het communicatiegeheim niet langer is gebonden aan specifieke communicatiemiddelen voorziet de nieuwe formulering in de bescherming van alle mogelijkheden voor communicatie, zowel de huidige als toekomstige (digitale) .

Het wetsvoorstel tot herziening van artikel 13 van de Grondwet strekt aldus tot modernisering met als doel om op adequate wijze het communicatiegeheim te beschermen, waar het gaat om privécommunicatie. Waar het de vraag is of het privécommunicatie betreft, is de gerichtheid van de communicatie bepalend. Het betreft bescherming van het communicatiegeheim tegen heimelijk inzage in haar inhoud door anderen waaronder de overheid en inclusief degenen die het communicatiemiddel beheren.

De voorgestelde wijziging heeft eveneens geleid tot een herbezinning over de duur van de bescherming. Voorheen was deze beperkt tot de transportfase (totdat de brief was bezorgd). In nieuwe situaties met elektronische telecommunicatie is de duur moeilijker af te bakenen omdat transport en opslag meestal geleidelijk in elkaar overgaan en een derde vaak ook de opslag van een

Lange Voorhout 7 • Postbus 30315, 2500 GH Den Haag
Telefoon: 070-3611420 • info@nvvr.org • www.nvvr.org

bericht beheert. De bescherming van het telecommunicatiegeheim dient zich volgens de wetgever uit te strekken over de gehele periode waarin een derde het bericht beheert en toegang heeft tot de inhoud daarvan.

Advisering

De NVvR onderschrijft het nut en de noodzaak van de bescherming van grondrechten in het huidige 'digitale tijdperk'. De technologische ontwikkelingen nopen tot de herziening van de thans verouderde regelgeving, teneinde de grondrechten van burgers optimaal te kunnen beschermen. De NVvR is dan ook verheugd dat het kabinet uitvoering heeft willen geven aan de aanbeveling van de Staatscommissie Grondwet om tot de onderhavige Grondwetswijziging over te gaan.

De NVvR wenst in haar advies op twee aspecten nader in te gaan. Het betreft in de eerste plaats de mate van rechtsbescherming van burgers bij het maken van inbreuk door de overheid op het hier bedoelde grondrecht. In de tweede plaats laat de NVvR zich uit over de regelingsopdracht aan de overheid die is vervat in het voorgestelde derde lid van artikel 13 Grondwet.

Rechtsbescherming

Het voorgestelde eerste lid van artikel 13 Grondwet houdt in dat iedereen het recht heeft op eerbieding van zijn brief- en telecommunicatiegeheim. Het gaat hier om de bescherming van een grondrecht. Dat impliceert dat een hoge mate van rechtsbescherming van de burgers tegen schending daarvan is vereist. Gelet hierop is de NVvR van mening dat bij het maken van elke inbreuk op het hierbedoelde grondrecht een rechterlijke toetsing vooraf door het verlenen van een machtiging op zijn plaats is. Bij de vaststelling door de rechter of artikel 13 Grondwet in een specifieke casus van toepassing is, heeft de rechter onder meer een oordeel te vormen over de gerichtheid van de communicatie. In de praktijk houden rechters en officieren van justitie reeds rekening met de gerichtheid van de communicatie; evenwel is een duidelijke begrenzing nodig. Immers, alle communicatiekanalen kunnen zowel voor gerichte als voor ongerichte communicatie gebruikt worden.

Op pagina 21 van de memorie van toelichting wordt gesteld dat de onderhavige Grondwetswijziging in feite gezien wordt als een codificatie op het niveau van de Grondwet van een aangelegenheid die op het niveau van de wet al is geregeld, aangezien het Wetboek van Strafvordering (hierna Sv) reeds voorschrijft dat een machtiging van de rechter is vereist voor het opnemen van telecommunicatie (art. 126m, 126t en 126zg Sv). Opmerking verdient hierbij dat het verankeren van een recht in de Grondwet daaraan het karakter van een 'grondrecht' toekent. Als gevolg hiervan worden aan de grondwettelijk verankerde rechten in feite hogere eisen gesteld in termen van waarborgen en rechtsbescherming. Gelet hierop heeft de grondwettelijke delegatie meer waarde. Deze meerwaarde komt aldus tot uitdrukking bij de voorwaarden tot het beperken van dit grondrecht.

In het licht van de snelheid van de technologische ontwikkelingen is het evenwel denkbaar dat het in de toekomst voor de rechtspraktijk van belang is de regelgeving op dit terrein met de nodige voortvarendheid aan te passen. De complexe en langdurige herzieningsprocedure van de Grondwet kan dit in de weg staan. De NVvR werpt de vraag op of het om die reden niet wenselijker moet worden geacht de rechterlijke toetsing langs de weg van delegatie naar een wet in formele zin in plaats van in artikel 13 van de Grondwet te regelen.

In het tweede lid wordt voorts voorgesteld dat beperking van dit recht tevens mogelijk is, in het belang van de nationale veiligheid, met machtiging van één of meer bij de wet aangewezen ministers.

De voorgestelde regeling betekent naar de mening van de NVvR op dit punt een verschraling van de huidige rechtsbescherming. Het wetsvoorstel schrijft in die gevallen voor dat in plaats van een

machtiging van de rechter een machtiging van de minister is vereist. Het argument dat aan deze wijziging ten grondslag ligt is dat het gaat om belangrijke beleidsbeslissingen die verband houden met de nationale veiligheid[1]: "De minister is in dezen beter geïnformeerd dan de rechter en kan tot een integrale afweging komen."

De NVvR adviseert negatief ten aanzien van deze wijziging. De NVvR acht het, vanuit rechtsstatelijk oogpunt bezien, noodzakelijk dat een onafhankelijke rechter de mogelijkheid krijgt om een afweging te maken of de beperking plaats dient te hebben. Vanuit het rechtsstatelijk oogpunt bezien wordt met de voorgestelde regeling het principe van checks en balances losgelaten. De mogelijkheid dat de minister deze bevoegdheid, zelfs in theorie, kan mandateren aan de ambtenaren van de AIVD creëert eveneens een onwenselijke situatie.
Kijkend naar de uitvoering, is de wijze waarop de exclusief daarvoor aangewezen kamer van de rechtbank Den Haag dergelijke zaken beoordeelt, niet gelijk te stellen met de wijze waarop de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) toezicht uitoefent. Conform artikel 64, tweede lid, van de Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv 2002) is de Commissie belast met het toezicht op de rechtmatigheid van de uitvoering van de handelingen verricht door de AIVD. Dat waarborgt op zichzelf niet dat elke concrete inbreuk op dit grondrecht tevoren door de commissie wordt getoetst, op de wijze waarop wordt getoetst bij rechterlijke machtiging. De NVvR is van mening dat onafhankelijk toezicht hiermee onvoldoende is gewaarborgd. Dit geldt zowel voor het briefgeheim als voor het telecommunicatiegeheim. De NVvR hecht eraan op te merken dat, zoals vermeld op pagina 22 van de memorie van toelichting, ook het afleggen van verantwoording aan het parlement een fundamenteel andere verantwoordelijkheid behelst dan een afweging in individuele gevallen door een onafhankelijke rechter, daar waar het gaat om een al dan niet gerechtvaardigde inbreuk op artikel 13 van de Grondwet.

Voorts is de formulering 'in het belang van de nationale veiligheid' naar de mening van de NvvR te ruim. De NVvR vraagt zich af in welke gevallen het vereiste van 'in het belang van de nationale veiligheid' als rechtvaardiging kan worden aangewend om inbreuk te maken op dit grondrecht van burgers. Dit pleit naar de mening van NVvR des te meer voor een wettelijke grondslag voor rechterlijke toetsing in plaats van een ministeriële toetsing . Volledigheidshalve verwijzen wij hierbij naar de beperkingsystematiek van het EVRM en de daarin geformuleerde doelcriteria voor het maken van inbreuk op de grondrechten.

De NVvR adviseert om van de toekenning van deze bevoegdheid aan de minister af te zien.

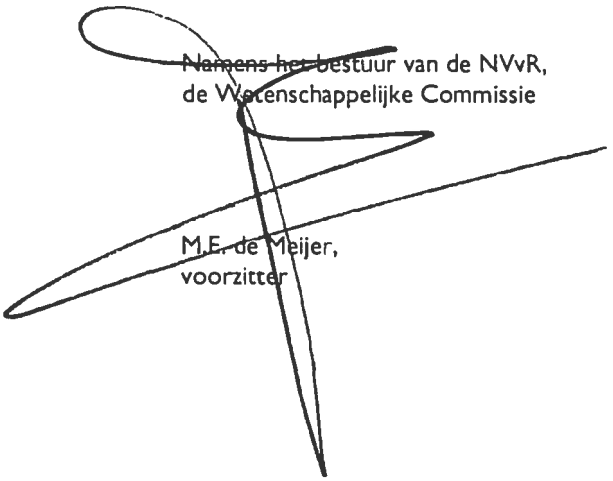
Regelingsopdracht

Ten aanzien van de regelingsopdracht aan de wetgever zoals vervat in het derde lid, ziet de NVvR meerwaarde ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg van de overheid, voor zover de overheid zich inspant voor een netneutraal internet. Verder is de NVvR van opvatting dat vastgehouden moet worden aan het feit dat de overheid in beginsel na interceptie van vertrouwelijke communicatie de betrokkene daarvan in kennis stelt. De NVvR constateert dat op pagina 26 van de memorie van toelichting in dit verband is gerefereerd aan de door de CTIVD gestelde vraag of de kosten van de tenuitvoerlegging van de notificatieplicht opwegen tegen de baten. Gelet op het belang van de onderhavige inbreuk op de persoonlijke levenssfeer meent de NVvR dat de notificatieplicht alleszins gerechtvaardigd is.

De NVvR adviseert in de regelingsopdracht aan de wetgever, die is vervat in het voorgestelde derde lid van artikel 13 , duidelijke doelcriteria op te nemen. Immers het moeten gerechtvaardigde belangen zijn waar het gaat om inperking en notificatie achteraf aan de burger.[2]

---

[1] Memorie van Toelichting bij het wetsvoorstel Wijziging artikel 13 Grondwet, pagina 22.
[2] Rapport Commissie Grondrechten in het Digitale Tijdperk (Commissie Franken), mei 2000, p. 157



Namens het bestuur van de NVvR,
de Wetenschappelijke Commissie

M.E. de Meijer,
voorzitter

PRIVACY FIRST

Postbus 71909
1008 EC Amsterdam
Tel. 020 - 8100279

Aan:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Plaatsvervangend Directeur Constitutionele Zaken en Wetgeving
Dhr. mr. W.J. Pedroli
Postbus 20011
2500 EA Den Haag

Uw ref.	:	2012-0000594504
Onze ref.	:	SPF-20121229
Datum	:	29 december 2012
Betreft	:	Commentaar Privacy First op concept-wetsvoorstel tot wijziging van art. 13 Grondwet

Geachte heer Pedroli,

Op 16 oktober jl. verzocht u Stichting Privacy First om een reactie te geven op het concept-wetsvoorstel tot wijziging van artikel 13 Grondwet. Privacy First is u erkentelijk voor uw verzoek en voorziet u hierbij graag van kritisch commentaar. Daarbij zij allereerst opgemerkt dat Privacy First de wens van dit kabinet om het huidige, archaïsche artikel 13 Grondwet te moderniseren volledig onderschrijft. Privacy First betreurt het echter dat het kabinet niet de kans heeft gegrepen om ook andere 'grondrechten in het digitale tijdperk' te vernieuwen en te versterken.

Positieve aspecten

In de optiek van Privacy First vormen het eerste en derde lid van het huidige concept-wetsvoorstel ter herziening van artikel 13 Grondwet krachtige ankerpunten voor een toekomstbestendig recht op vertrouwelijke communicatie. Het eerste lid moderniseert terecht het oude brief-, telefoon- en telegraafgeheim tot een techniekonafhankelijk (of techniekneutraal) brief- en telecommunicatiegeheim. Het derde lid vormt een juiste waarborg voor de horizontale uitwerking hiervan. Privacy First onderschrijft bovendien de ruime interpretatie die in de concept-memorie van toelichting (MvT) aan diverse relevante begrippen gegeven wordt. Het tweede lid van het concept-wetsvoorstel bevat echter een systematische disbalans die onze maatschappij in minder democratische tijden uit het rechtsstatelijke lood zou kunnen doen slaan. Het is dan ook met name dit tweede lid waarop de kritiek van Privacy First zich richt. Andere punten van kritiek betreffen de notificatieplicht en verkeersgegevens alsmede het ontbreken van een rechtsvergelijkende paragraaf in de MvT.

Rechterlijke machtiging en nationale veiligheid

Terecht stelt de MvT dat "in het licht van artikel 13 (...) de bescherming van de burger tegen inbreuken van de overheid voorop [staat], met name in het licht van

optreden van politie en inlichtingendiensten. (...) Het stellen van de eis van een rechterlijke machtiging in de Grondwet geeft een sterke en duidelijke rechtsstatelijke waarborg."[1] Het is dan ook onbegrijpelijk dat in het tweede lid van het concept-wetsvoorstel het domein van de nationale veiligheid van rechterlijk toezicht wordt uitgezonderd. Daar waar de machtsconcentratie het hoogst is, dienen immers de juridische *checks & balances* het krachtigst te zijn om (toekomstig) machtsmisbruik te voorkomen. In het licht van de Europese geschiedenis is de uitzondering in lid 2 zelfs volstrekt onverantwoord: ook in onze contreien is een democratische rechtsstaat helaas geen statisch gegeven. Daarnaast geeft e.e.a. een gevaarlijk signaal aan het buitenland. De uitzondering in lid 2 acht Privacy First bovendien onverstandig met het oog op mogelijke technologische ontwikkelingen in de (verre) toekomst.[2] Hetzelfde geldt in verband met de (verdere) oprekking van het begrip "nationale veiligheid". Ook in de toekomst dient de Nederlandse bevolking tegen willekeurige inbreuken op het communicatiegeheim beschermd te zijn; de huidige formulering van lid 2 biedt hiertoe geen enkele garantie.

Het toevoegen van een extra 'rechterlijke laag' zou het huidige stelsel van intern en extern toezicht op de inlichtingen- en veiligheidsdiensten (en daarmee de democratische rechtsstaat) versterken. Het systeem van rechterlijk toezicht in een land als Canada kan in dit opzicht een bron van inspiratie vormen. Een dergelijke rechterlijke *check* zou tevens in lijn zijn met de jurisprudentie van het Europees Hof voor de Rechten van de Mens:

> *"The Court has indicated, when reviewing legislation governing secret surveillance in the light of Article 8 [ECHR], that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."*[3]

In het licht hiervan is de huidige formulering van lid 2 niet opportuun. Privacy First adviseert dan ook om dit lid als volgt te herzien:

> *"Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter ~~of, in het belang van de nationale veiligheid, met machtiging van één of meer bij de wet aangewezen ministers~~."*
> [doorstreping Privacy First]

Als eventueel alternatief voor de invoering van rechterlijk toezicht in het veiligheidsdomein adviseert Privacy First om de bestaande Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) te *upgraden* tot een krachtiger onafhankelijk toezichtsorgaan *à la* het Belgische of Duitse model, met algehele, verplichte toetsing *vooraf* i.p.v. steekproefsgewijs toezicht *achteraf*.

---

[1] MvT, pp. 18, 20.

[2] Vergelijk MvT, p. 11, 1e alinea.

[3] EHRM 22 nov. 2012, *Telegraaf vs. Nederland* (Appl.no. 39315/06), r.o. 98. Vergelijk tevens *ibid.*, r.o. 98-102.

Notificatieplicht

Een tweede punt van kritiek betreft het ontbreken van expliciete grondwettelijke vermelding van een notificatieplicht bij inbreuken op het brief- en telecommunicatiegeheim. Een notificatieplicht versterkt immers de rechtsbescherming voor burgers en draagt bij aan correcte naleving van de wet door de overheid, ook in het veiligheidsdomein. Evenals rechterlijke machtiging biedt dit de beste garanties tegen misbruik op korte én lange termijn.

Verkeersgegevens

In de optiek van Privacy First dienen ook verkeersgegevens onder de reikwijdte van artikel 13 Grondwet te vallen. Deze gegevens zien immers vaak mede op de *inhoud* van communicatie; dit blijkt zelfs met zoveel woorden uit de MvT zelf, waar terecht SMS en de onderwerp-regel van email als voorbeelden worden genoemd.[1] Hetzelfde geldt bijvoorbeeld voor zoekopdrachten in zoekmachines. Daarnaast kan uit verkeersgegevens *in combinatie met andere* (al dan niet *real-time* verzamelde) gegevens alsnog de inhoud van communicatie tussen individuen en/of bedrijven worden afgeleid. Een krachtig regime van artikel 13 Grondwet in combinatie met rechterlijk toezicht is dus ook hier geboden.

Rechtsvergelijking

Tenslotte mist Privacy First in de huidige MvT een rechtsvergelijkende paragraaf waarin het huidige artikel 13 Grondwet vergeleken wordt met grondwettelijke *best practices* uit landen met hetzij een *civil law*, hetzij een *common law* traditie. Met een nieuw artikel 13 Grondwet als internationale *state-of-the-art* zou Nederland zich bovendien positief kunnen onderscheiden en haar vroegere positie als mensenrechtelijk gidsland enigszins kunnen heroveren.

Privacy First hoopt u met dit advies van dienst te zijn. Desgevraagd zijn wij graag tot een nadere toelichting op bovenstaande punten bereid.

Hoogachtend,

Stichting Privacy First

mr. Vincent A. Böhre
director of operations

[1] MvT, p. 18.

Openbaar Ministerie
College van Procureurs-Generaal
Voorzitter

Postbus 20305 2500 EH Den Haag

Prins Clauslaan 16
2595 AJ Den Haag
Telefoon +31 (0)70 339 96 00
telefax +31 (0)70 339 98 51

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Constitutionele Zaken en Wetgeving
t.a.v. de heer W.J. Pedroli
Postbus 20011
2500 EA 'S-GRAVENHAGE

Onderdeel	Beleid & Strategie
Contactpersoon	
Doorkiesnummer(s)	
E-mail	
Datum	07-02-2013
Ons kenmerk	PaG/B&S/16653
Uw kenmerk	312249
Onderwerp	Advies conceptwetsvoorstel tot wijziging van artikel 13 Grondwet

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen

Geachte heer Pedroli,

Bij brief van 24 oktober 2012 heeft u namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties het College van procureurs-generaal gevraagd te adviseren over een conceptwetsvoorstel tot wijziging van artikel 13 van de Grondwet.
Het wetsvoorstel strekt ertoe het huidige artikel 13 grondwet, waarin het brief- telefoon- en telegraafgeheim is neergelegd, te moderniseren en uit te breiden naar alle moderne vormen van communicatie.

Het College heeft met belangstelling kennis genomen van het onderhavige wetsvoorstel. Terecht wordt geschetst dat de mate van bescherming die artikel 13 Grondwet biedt op dit moment afhankelijk is van het gebruikte middel. De communicatie per brief is op grondwettelijk niveau beter beschermd dan communicatie per telefoon omdat in het huidige artikel 13 Grondwet voor de eerste een last van de rechter is voorgeschreven en voor de laatste niet.
In lagere wetgeving, zoals het Wetboek van Strafvordering, wordt de privé-communicatie al wel op gelijk niveau beschermd. Voor een inbreuk op het briefgeheim, het onderscheppen van communicatie van telefoon- of internetverkeer, of het opvragen van bijvoorbeeld emailberichten is op grond van het Wetboek van Strafvordering een machtiging van de rechter-commissaris noodzakelijk. Deze regeling is in overeenstemming met artikel 8 van het EVRM. Met de voorgestelde wijziging van de Grondwet wordt dan ook geen wijziging van de huidige praktijk beoogd.

Het College is het eens met de benadering dat voor de verschillende vormen van communicatie dezelfde grondwettelijke bescherming wordt gecreëerd en dat het nieuwe artikel 13 Grondwet techniekonafhankelijk wordt geformuleerd. Op deze wijze wordt duidelijk wat het object van grondwettelijke bescherming dient te zijn: de privé-communicatie. Dit wordt ook uitstekend geïllustreerd in hoofdstuk 2 van de memorie van toelichting, waar de inhoud en reikwijdte van het brief- en telecommunicatiegeheim wordt besproken.

Het College signaleert echter dat een voorbeeld in de memorie van toelichting minder gelukkig is gekozen. Gesteld wordt dat voor het natrekken van ingetypte zoekvragen in een internetzoekmachine een machtiging van de rechter noodzakelijk is. Het College merkt op dat het bij een aanbieder van een telecommunicatiedienst opvragen van gegevens die betrekking hebben op een zoekvraag in een zoekmachine op grond van artikel 126ng, lid 1 jo126nd Sv door de officier van justitie kan geschieden. Hiervoor is geen machtiging van de rechter-commissaris vereist.
In dit verband kan een vergelijking worden gemaakt met het opvragen van gegevens bij een bibliotheek. Op grond van artikel 126nd Sv kan de officier van justitie bij de bibliotheek gegevens opvragen die betrekking hebben op het lenen van boeken door de verdachte. Inhoudelijk ziet het College hier geen groot verschil.
Een iets ander voorbeeld is het vorderen van gegevens bij een bank. Op grond van artikel 126nd Sv kan de officier van justitie van een bank vorderen dat opgeslagen of vastgelegde gegevens, zoals rekeningafschriften van een cliënt, worden verstrekt. Op deze rekeningafschriften zullen ook gegevens voorkomen die met behulp van internetbankieren zijn gegenereerd. Maar ook in deze situatie is een machtiging van de rechter-commissaris niet vereist.

Artikel 13 van de Grondwet is een kader stellend artikel. In lagere wetgeving wordt de bescherming van het brief- en telecommunicatiegeheim en de beperking nader vorm gegeven. Voorts wordt met de modernisering van artikel 13 van de Grondwet geen wijziging van de huidige praktijk beoogd.
Het College adviseert daarom om het noemen van voorbeelden in de memorie van toelichting te beperken tot die gevallen waarin ook onder het huidige recht een rechterlijke toetsing noodzakelijk is. Daarmee kan worden voorkomen — omdat het voorbeeld in de memorie van toelichting met name wordt genoemd — dat op een later moment in lagere wetgeving een rechterlijke toets wordt opgenomen in gevallen waar het in de huidige praktijk voldoende wordt geacht dat de officier van justitie beveelt gegevens te verstrekken.
Ten overvloede merkt het College op dat door de regering, zittende magistratuur, politie en openbaar ministerie op dit moment hard wordt gewerkt aan het terugdringen van de administratieve lastendruk. In dit kader wordt ook gekeken naar alle gevallen waarin een machtiging van de rechter wordt voorgeschreven. Dit project

kan worden bemoeilijkt doordat in een memorie van toelichting bij een grondwetswijziging voorbeelden van rechterlijke toetsing worden genoemd, waarvan in de praktijk nog moet blijken of deze toets wel noodzakelijk is.

Hoogachtend,
Het College van procureurs-generaal

H.J. Bolhaar

Documentbeheer

EINDE DOCUMENT

2712201200394 1

Agentschap Telecom
Ministerie van Economische Zaken

> Retouradres Postbus 450 9700 AL Groningen

Ministerie van Binnenlandse Zaken
Directie Constitutionele Zaken en Wetgeving

Postbus 20011
2500 EA Den Haag

Emmasingel 1
9726 AH Groningen
Postbus 450
9700 AL Groningen
T (050) 587 74 44
F (050) 587 74 00
www.agentschaptelecom.nl
info@agentschaptelecom.nl

Contactpersoon

VERZONDEN 20 DEC 2012

Datum

Ons kenmerk
AT-EZ/6781269

Uw kenmerk
2012-0000611604

Betreft Consultatie concept wetsvoorstel tot wijziging van artikel 13 Grondwet

Geachte heer Pedroli,

Op 24 oktober 2012 heb ik uw brief inzake de consultatie van het concept wetsvoorstel tot wijziging van artikel 13 Grondwet ontvangen. Graag reageer ik hierbij op uw verzoek om voor 1 januari 2013 een reactie te sturen.

U vraagt in uw brief bijzondere aandacht voor de volgende twee punten. Het eerste punt betreft uw vraag over de mogelijke gevolgen dat, naast de hoofdregel dat een beperking van het brief- en telecommunicatiegeheim in beginsel een machtiging van de rechter vereist, bij uitzondering op deze hoofdregel een beperking in het kader van nationale veiligheid is toegestaan met machtiging van één of meer ministers. Wat betreft deze uitzondering kan voor Agentschap Telecom de volgende situatie aan de orde zijn. In artikel 13.2 van de Telecommunicatiewet (hierna: Tw) is bepaald dat een telecomaanbieder moet voldoen aan een bevel tot aftappen. Krachtens de artikelen 15.1, eerste lid, Tw en volgende is Agentschap Telecom belast met het toezicht hierop en de handhaving hiervan. Indien een telecomaanbieder bezwaar maakt of beroep instelt tegen een door het agentschap opgelegde sanctie (boete en/of last onder dwangsom) op grond van het geen gevolg geven aan een bevel tot het aftappen van een telefoon dan kan de aanbieder in dat verband aanvoeren dat in strijd met artikel 13 van de Grondwet géén rechtelijke machtiging is afgegeven, omdat naar zijn oordeel de uitzondering van nationale veiligheid niet van toepassing is. Agentschap Telecom zal dan dienen te onderbouwen waarom er sprake is van een gerechtvaardigde beperking van het telecommunicatiegeheim op grond van nationale veiligheid. Dit laatste is echter niet wenselijk aangezien het agentschap niet over informatie zal beschikken waarom de nationale veiligheid in het geding is, waardoor het sanctiebesluit door het agentschap in bezwaar en beroep niet overeenkomstig de Algemene wet bestuursrecht kan worden gemotiveerd. Agentschap Telecom adviseert om in de toelichting hier aandacht aan te besteden.

Het tweede punt behelst de opdracht aan de wetgever om regels te stellen ter bescherming van het brief- en telecommunicatiegeheim en de vraag in hoeverre dit een meerwaarde heeft ter ondersteuning van het brief- en telecommunicatiegeheim als voorwerp van aanhoudende zorg voor de overheid. Deze opdracht aan de wetgever heeft meerwaarde, aangezien daarmee aan het grondrecht horizontale werking kan worden gegeven. Indien deze vraag daarnaast

zo kan worden begrepen dat onder bescherming tevens valt het stellen van voorwaarden waaronder gerechtvaardigd een inbreuk kan worden gemaakt op het brief- en telecommunicatiegeheim, dan is Agentschap Telecom van mening dat het van belang is dat de wetgever daarover regels stelt. Hierbij denk ik bijvoorbeeld aan artikel 13.2, derde lid, Tw waarin is bepaald:
"Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen organisatorische en personele maatregelen en te treffen voorzieningen [door aanbieders van openbare telecommunicatienetwerken] met betrekking tot aftappen."

Naast de reactie op bovenstaande punten zou ik graag de volgende opmerkingen willen maken.

Opmerking 1:
In de memorie van toelichting is op pagina's 17 en 18 vermeld:
"Aandacht verdient evenwel dat de inhoud van telecommunicatie in technische zin soms ook als een verkeersgegeven wordt gezien. Zo wordt het onderwerp van een e-mail in technische zin wel tot de verkeersgegevens betreffende die e-mail gerekend. Maar in juridische zin valt het onderwerp van een e-mail onder de reikwijdte van artikel 13 omdat dat onderwerp betrekking heeft op de inhoud van de e-mail. [...] Verkeersgegevens die niet mede betrekking hebben op de inhoud van telecommunicatie vallen echter buiten de reikwijdte van artikel 13."

In artikel 11.1, onder b, Tw zijn verkeersgegevens als volgt gedefinieerd:
"verkeersgegevens: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan".

Indien de definitie van de Tw wordt aangehouden kan er geen sprake van zijn dat verkeersgegevens ook betrekking hebben op de inhoud en kunnen verkeersgegevens derhalve niet vallen onder de reikwijdte van artikel 13 Grondwet. Daarbij is het dan ook niet relevant, indien de definitie van de Tw wordt aangehouden, om in paragraaf 6.4 van de toelichting in te gaan op hoe met verkeersgegevens dient te worden omgegaan door telecomaanbieders (artikel 11.5 Tw). Immers hetgeen daarover wordt opgemerkt in paragraaf 6.4 heeft gezien voormelde definitie alleen betrekking op de bescherming van de persoonlijke levenssfeer en niet op de bescherming van het brief- en telecommunicatiegeheim. Agentschap Telecom adviseert gezien het voorgaande om de reikwijdte van artikel 13 Grondwet niet zodanig uit te breiden dat ook verkeersgegevens daaronder gaan vallen, aangezien dit ertoe zou leiden dat aan verkeersgegevens een ruimere betekenis wordt toegekend dan juridisch plus technisch gebruikelijk is en dat de definitie van verkeersgegevens in de Tw aangepast dient te worden.

Opmerking 2:
Op pagina 25 van de toelichting is opgenomen:
"De Telecommunicatiewet richt zich exclusief op normadressaten die een openbaar karakter hebben. Elektronische netwerken en elektronische diensten met een besloten karakter vallen buiten het bereik van de Telecommunicatiewet. [...] Met de constatering dat de Telecommunicatiewet enkel geldt voor openbare netwerken en diensten is het communicatieverkeer dat plaatsvindt in netwerken en diensten met een besloten karakter evenwel niet vogelvrij voor wat betreft hun brief- en telecommunicatiegeheim."

En op pagina 35 van de toelichting is vermeld:

"Gesloten elektronische netwerken zoals bijvoorbeeld netwerken van werkgevers vallen evenwel niet onder de reikwijdte van de Telecommunicatiewet; zij worden thans bestreken door de Wbp en de relevante bepalingen in het BW."

Ons kenmerk
AT-EZ/6781269

De Tw ziet niet alleen op netwerken en diensten met een openbaar karakter. Voor ieder gebruik van frequenties (openbaar of niet-openbaar) is een vergunning van het agentschap vereist, tenzij er een vrijstelling van de vergunningplicht geldt. Een voorbeeld van een niet-openbaar elektronisch netwerk waarop de Tw van toepassing is, is het vergunningvrij frequentiegebruik door basisstations met bijbehorende telefoons voor onder meer netwerken van werkgevers (zie artikel 3.4, eerste lid, onder a Tw, juncto artikel 2, tweede lid, onder o en artikel 8a van de Regeling gebruik van frequentieruimte zonder vergunning 2008). Terzijde, wanneer artikel 13.7 Tw in werking treedt kan er ook voor aanbieders van niet-openbare telecommunicatiediensten de verplichting gaan gelden dat deze dienst aftapbaar moet zijn. Graag zou Agentschap Telecom zien dat de toelichting op basis van het voorgaande wordt aangepast.

Opmerking 3:
In de toelichting is op pagina 34 vermeld:
"Aanbieders mogen aldus op grond van dit tweede lid [van artikel 18.13 Tw] geen kennis nemen van de inhoud van de communicatie of verkeersgegevens verwerken, tenzij dit uitdrukkelijk bij of krachtens de Tw is toegestaan."

Hetgeen in de toelichting is opgenomen ten aanzien van verkeersgegevens betreft de bescherming van de persoonlijke levenssfeer. Agentschap Telecom wijst erop dat artikel 18.13 Tw zowel bescherming van de persoonlijke levenssfeer als bescherming van het brief- en telecommunicatiegeheim betreft, maar dat in paragraaf 6.4 dit van elkaar dient te worden gescheiden en alleen bescherming van het brief- en telecommunicatiegeheim relevant is.
Daarnaast is het telecomaanbieders op grond van de Tw niet toegestaan om kennis te nemen van de inhoud van de communicatie, alleen opsporingsambtenaren zijn bevoegd om hiervan kennis te nemen in het kader van een strafrechtelijk onderzoek (zie artikelen 13.2 en 13.2b Tw). Agentschap Telecom adviseert dat de toelichting overeenkomstig het voorgaande wordt aangepast.

Opmerking 4:
In paragraaf 6.4 van de toelichting wordt op pagina 34 ingegaan op locatiegegevens (artikel 11.5a Tw). Agentschap Telecom meent dat dit niet relevant is en adviseert dit te verwijderen, aangezien locatiegegevens niet vallen onder de reikwijdte van artikel 13 Grondwet. Deze gegevens vallen onder de bescherming van de persoonlijke levenssfeer.

Voor vragen over deze brief kunt u contact opnemen met mevrouw Oostland. Zij is bereikbaar via telefoonnummer 050 - 5877121. Vooralsnog ga ik er vanuit dat ik u hierbij voldoende heb geïnformeerd.

Hoogachtend,

mr. drs. P.A. Spijkerman
Directeur-hoofdinspecteur
Agentschap Telecom

Documentbeheer

EINDE DOCUMENT

1112012000350

Vereniging van Nederlandse Gemeenten

Ministerie van Binnenlandse Zaken enKoninkrijksrelaties (BZK)
De heer dr. R.H.A. Plasterk
Postbus 20011
2500 EA 'S-GRAVENHAGE

doorkiesnummer	uw kenmerk	bijlage(n)
(070) 373 8211	2012-0000581107	-
betreft	**ons kenmerk**	**datum**
Consultatie concept wetsvoorstel tot wijziging van artikel 13 Grondwet	ECGR/U201201782	16 november 2012

Geachte heer Plasterk,

Wij hebben uw brief inzake het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet (brief d.d. 1 november, kenmerk 2012-0000581107) in goede orde ontvangen. U stelt ons daarbij in de gelegenheid om op het wetsvoorstel te reageren.

We hebben kennis genomen van het wetsvoorstel dat ertoe strekt de reikwijdte van de onschendbaarheid van het brief-, telefoon- en telegraafgeheim dat in artikel 13 Grondwet is neergelegd, uit te breiden naar alle communicatiemiddelen. We onderschrijven een aanpassing van het artikel vanwege de hoge vlucht die het gebruik van elektronische communicatiemiddelen heeft genomen in de digitale informatiesamenleving. Modernisering van het huidige artikel, waarin enkel wordt gerefereerd aan de specifieke communicatiemiddelen brief, telegraaf en telefoon, is gewenst teneinde tot een techniekonafhankelijke bescherming te komen.

Gelet echter op het geringe gemeentelijke belang bij het conceptwetsvoorstel, hebben wij besloten inhoudelijk niet (verder) op het voorstel te reageren. We vertrouwen op uw begrip voor dit standpunt.

Hoogachtend,
Vereniging van Nederlandse Gemeenten

drs. C.J.G.M. de Vet
lid directieraad