

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 Mens² 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 karakter¹⁵ 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 noodzakelijkheids criterium (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 mogelijksterwils minder bescherming zou kunnen ontleen 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.cbplib.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.cbplib.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://cbplib.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.cbplib.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 ontlelen 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 af luisteren 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”*, (onderstreept 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.