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 De minister van Veiligheid en Justitie

DATUM 10 februari 2015
ONS KENMERK z2014-00885
CONTACTPERSOON

UW BRIEF VAN 18 november 2014
UW KENMERK

ONDERWERP Wetgevingsadvies Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische telecommunicatiediensten

Geachte ,

Bij brief van 18 november 2014 heeft u, mede namens de minister van Economische Zaken, het College bescherming persoonsgegevens (CBP) op grond van het bepaalde in artikel 51, tweede lid van de Wet bescherming persoonsgegevens (Wbp) gevraagd te adviseren op het wetsvoorstel Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische communicatiediensten (hierna: het wetsvoorstel).

Het wetsvoorstel was ter consultatie opengesteld via internet van 18 november tot en met 31 december 2014. Na ommekomst van de consultatietermijn heeft het ministerie van Veiligheid en Justitie het CBP bericht dat er geen voor het CBP relevante wijzigingen zullen worden doorgevoerd in het wetsvoorstel. Het CBP adviseert derhalve op het wetsvoorstel zoals dat op 18 november 2014 aan het CBP is voorgelegd en voldoet hiermee aan uw verzoek.

Inhoud van het wetsvoorstel

Het wetsvoorstel betreft een aanpassing van de bestaande bewaarplicht voor telecommunicatiegegevens van zowel telefoon- als internetverkeer. De directe aanleiding is het arrest van het Hof van Justitie van de Europese Unie (hierna: het Hof) van 8 april 2014 in de gevoegde zaken Digital Rights Ireland en Seitlinger (hierna: het Hofarrest) waarin de Europese dataretentierichtlijn 2006/24/EG ongeldig is verklaard.

De Nederlandse regering heeft de afdeling Advisering van de Raad van State gevraagd om voorlichting te geven over de gevolgen van het Hofarrest voor de Nederlandse implementatiewetgeving van de ongeldig verklaarde Europese richtlijn (de Wet bewaarplicht telecommunicatiegegevens uit 2009). De Raad van State concludeert dat het enkele feit dat de Europese richtlijn ongeldig is verklaard geen gevolgen heeft voor de geldigheid van de Nederlandse implementatiewetgeving. Tegelijkertijd stelt de Raad dat aangenomen moet worden dat ook de implementatiewetgeving, die materieel grotendeels overeenkomt met de ongeldig verklaarde richtlijn, strijdig is met artikel 7 en 8 van het Handvest van de Grondrechten van de

Europese Unie (hierna: het Handvest). De Wet bewaarplicht telecommunicatiegegevens zal daarom in elk geval moeten worden aangepast om te voldoen aan de in het Hofarrest gestelde voorwaarden.

Het wetsvoorstel behelst geen intrekking van de bewaarplicht telecommunicatiegegevens, maar omvat aanpassingen op de volgende punten.

1. Introductie van een voorafgaande toetsing door een rechter-commissaris op vorderingen van officieren van justitie tot verstrekking van historische telecommunicatiegegevens.
2. Introductie van een onderscheid tussen een bewaartermijn van twaalf maanden voor telefoniegegevens en de termijn van raadpleging ervan tussen de zes en twaalf maanden, afhankelijk van de aard van het misdrijf.
3. Introductie van een verplichting tot opslag en verwerking van de gegevens binnen de Europese Unie.
4. Introductie van een recht op toegang tot de bewaarde gegevens door de toezichthouder.
5. Aanpassing van de bijlage met de specificatie van de te bewaren gegevens.

Beoordeling van het voorstel

Het CBP heeft de inhoud van het wetsvoorstel getoetst aan de normen van noodzakelijkheid, subsidiariteit en proportionaliteit, afkomstig uit artikel 8 van het Europees Verdrag van de Rechten van de Mens, en de artikelen 7 en 8 van het Handvest. Zoals in de bijlage bij deze brief is uiteengezet, luidt zijn oordeel en vervolgens zijn advies hierover als volgt.

Het CBP constateert dat de feitelijke onderbouwing in het wetsontwerp van de noodzaak om de telecommunicatiegegevens van *de facto* elke Nederlander gedurende zes tot twaalf maanden te bewaren, tekort schiet. Het wetsvoorstel bevat geen systematisch, met het gewicht van de voorgestelde maatregel overeenkomend, betoog van de noodzaak voor deze bewaarplicht. Dit terwijl de opsporingsautoriteiten ruim vier en half jaar ervaring hebben kunnen opdoen met de bewaarde persoonsgegevens sinds de inwerkingtreding van de Wet bewaarplicht telecommunicatiegegevens. Het wetsvoorstel bevat in het geheel geen uitwerking van de subsidiariteitstoets.

Ten aanzien van de evenredigheid van het wetsvoorstel stelt het CBP vast dat er geen wezenlijke veranderingen worden aangebracht in het principe van een algemene bewaarplicht. De bewaarplicht wordt niet ingekaderd en kán volgens de regering ook niet worden ingekaderd tot enkel die gegevens die noodzakelijk zijn voor het bestrijden van zware criminaliteit. De inbreuk op de artikelen 7 en 8 van het Handvest is daarmee te groot en voldoet niet aan het proportionaliteitsvereiste van artikel 8 EVRM.
Ook ten aanzien van de naleving van de notificatieplicht, de controle op het gebruik van de bewaarde gegevens en het ontbreken van uitzonderingen voor mensen met een beroepsgeheim voldoet het wetsvoorstel niet aan de proportionaliteitsvereisten.

Ten slotte beoordeelt het CBP het door de regering beoogde onderscheid tussen het bewaren van gegevens en het gebruik ervan. Dit onderscheid leidt niet tot beëindiging van de geconstateerde onevenredigheid en daarmee onrechtmatigheid van een algemene bewaarplicht verkeersgegevens. In zijn algemeenheid merkt het CBP in dit verband op dat noch in internationale verdragen, noch in de Wet bescherming persoonsgegevens ruimte is te vinden voor dit beoogde onderscheid.

Advies

Het CBP heeft bezwaar tegen het voorstel van wet en adviseert u dit niet in te dienen.

Openbaarmaking

Aangezien het wetsvoorstel in openbare consultatie is gegeven, is het CBP voornemens het onderhavige wetgevingsadvies op of na 12 februari 2015 openbaar te maken.

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

DATUM 10 februari 2015
ONS KENMERK z2014-00885

Bijlage bij de brief van het College bescherming persoonsgegevens van 10 februari 2015 inzake het conceptwetsvoorstel Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische communicatiediensten

1. Inhoud van het wetsvoorstel

Artikel I van het wetsvoorstel betreft een wijziging van de Telecommunicatiewet. Hierin wordt vastgelegd dat telecomaanbieders verplicht zijn de door de aangepaste Wet bewaarplicht telecommunicatiegegevens vereiste gegevens gedurende zes dan wel twaalf maanden te bewaren teneinde te kunnen voldoen aan een vordering door de opsporingsdiensten. Tevens wordt vastgelegd dat de gegevens dienen te worden opgeslagen en verwerkt in Nederland, of in elk geval in een van de lidstaten van de Europese Unie.

Artikel I, onderdeel E biedt het Agentschap Telecom in de toekomst de mogelijkheid de gegevens inhoudelijk te controleren, onder meer om te kunnen nagaan of aan de verwijderplicht is voldaan.

Artikel I, onderdeel F bevat een wijziging van de bijlage bij artikel 13.2a van de Telecommunicatiewet, waarin de lijst met gegevens die dient te worden bewaard is vastgelegd. Er wordt een aantal te bewaren gegevens geschrapt uit de lijst (waaronder MMS en het gebruik van e-mail over internet). Daarnaast wordt de bewaarplicht voor Voice-over-IP telefoondiensten over een vast of mobiel netwerk verruimd van zes naar twaalf maanden. Ten slotte wordt de omschrijving van de bij het IP-adres te bewaren gegevens aangepast en wordt vastgelegd dat het last Cell ID (locatiegegeven afgeleid van de mast bij het beëindigen van een gesprek) niet hoeft te worden bewaard.

Artikel II van het wetsvoorstel behelst een aanpassing van de aan de bewaarplicht gelieerde bepalingen uit het Wetboek van Strafvordering. Een vordering van de gegevens door de officier van justitie wordt volgens deze bepalingen afhankelijk gemaakt van voorafgaande machtiging door de rechter-commissaris. De toegang tot de bewaarde telefoniegegevens (inclusief Voice-over-IP over vaste of mobiele netwerken) wordt gedifferentieerd, afhankelijk van de aard van het misdrijf. In beginsel geldt een termijn van zes maanden; alleen bij de opsporing en vervolging van strafbare feiten waarop een vrijheidsstraf van acht jaar is gesteld, mogen de gegevens die gedurende de volledige bewaartermijn zijn vastgelegd, worden gevorderd. Ten aanzien van internetgegevens wordt geen onderscheid aangebracht.

2. Beoordeling van het wetsvoorstel

2.1 Noodzakelijkheid van een algemene bewaarplicht van 6-12 maanden

In het arrest van 8 april 2014 heeft het Hof van Justitie van de Europese Unie (hierna: het Hof) geoordeeld dat de bewaarplicht, zoals deze destijds is vastgesteld door de Europese wetgever, in strijd is met artikel 7 en 8 van het Handvest.

De Nederlandse bewaarplicht is niet alleen ingevoerd op basis van de Richtlijn dataretentie, maar ook op de voet van artikel 15(1) van de ePrivacy Richtlijn. Dit biedt lidstaten de mogelijkheid nationale bewaarplichten in te voeren in het belang van de staatsveiligheid en voor het voorkomen, opsporen en vervolgen van strafbare feiten, mits deze wetgeving een noodzakelijke, passende en proportionele maatregel is in een democratische samenleving. De richtlijn schrijft voor dat dergelijke maatregelen moeten voldoen aan de algemene beginselen van het gemeenschapsrecht, inclusief het bepaalde in artikelen 6(1) en (2) van het Europees Verdrag, waaruit naleving van artikel 8 EVRM volgt. Nadien is het Handvest aangenomen. Op grond van artikel 51 van het Handvest is het Handvest ook van toepassing op nationale handelingen binnen het toepassingsgebied van het recht van de Unie. Daarom dient de nationale wetgeving te voldoen aan het bepaalde in artikel 7 en 8 van het Handvest. Dit wordt door de regering ook erkend in de beleidsbrief aan de Kamer[1] en in de Memorie van Toelichting bevestigd.[2]

Het Hof schrijft dat op grond van artikel 52 van het Handvest beperkingen kunnen worden gesteld aan de rechten op de persoonlijke levenssfeer en de bescherming van persoonsgegevens, zoals vastgelegd in artikel 7 en 8 van het Handvest. Dit kan echter alleen, wanneer deze beperkingen "*noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden*".[3] Het Hof overweegt dat het materiële doel van de dataretentierichtlijn – het onderzoek, de opsporing en de vervolging van ernstige criminaliteit – gezien kan worden als een doel van algemeen belang, omdat deze gegevens in de woorden van de Raad justitie en binnenlandse zaken van 19 december 2002 "*een waardevol instrument vormen bij het voorkomen van strafbare feiten en het bestrijden van criminaliteit, met name van de georganiseerde misdaad.*"[4] Daarmee stelt het Hof vast dat het gebruik van telecommunicatiegegevens door politie en justitie als zodanig niet strijdig is met het Handvest. Op het punt van de noodzaak van het bewaren van de telecommunicatiegegevens voor de strijd tegen de georganiseerde criminaliteit schrijft het Hof in het arrest dat het "*weliswaar van primordiaal belang is om de openbare veiligheid te waarborgen*", maar dat "*een dergelijke doelstelling van*

[1] Bijlage Reactie van het Kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie van 17 november 2014 (hierna: Beleidsbrief Kabinet) bij *Kamerstukken II* 2013/14, 33542, nr. 16, 27 november 2014, p. 7-8

[2] *Kamerstukken II* 2013/14, 33542, nr. 16, 27 november 2014 (hierna: Memorie van Toelichting), p. 7: "*Toetsing van de Wet bewaarplicht telecommunicatiegegevens aan het Handvest leidt tot de conclusie dat deze wet moet worden aangepast.*"

[3] Hofarrest, paragraaf 38.

[4] Hofarrest, paragraaf 43.

algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd."[5]

De regering stelt in haar beleidsbrief over de bewaarplicht overtuigd te zijn "*van het belang en de onmisbaarheid van een bewaarplicht voor telecommunicatiegegevens. Met een bewaarplicht wordt zeker gesteld dat bepaalde telecommunicatiegegevens beschikbaar zijn voor de opsporing en vervolging van ernstige strafbare feiten."*[6] Volgens de regering is de *essentie van de bewaarplicht (...). dat bepaalde telecommunicatiegegevens beschikbaar moeten zijn voor de opsporing van ernstige misdrijven. Als de gegevens voor dat doel strikt noodzakelijk zijn, dan is bewaring daarvan aan de orde* ."[7] In de Memorie van Toelichting schrijft de regering: "*De regering is dan ook overtuigd van het belang en de onmisbaarheid van een bewaarplicht voor telecommunicatiegegevens voor de opsporing en vervolging van ernstige misdrijven en stelt daarom voor deze verplichting te handhaven.*"[8]

Enkel het algemeen belang van de beschikbaarheid van telecommunicatiegegevens voor de opsporing rechtvaardigt op zich nog niet de noodzaak voor een algemene bewaarplicht van 6 tot 12 maanden. De regering lijkt in de beleidsbrief een doelredenering te gebruiken: als bepaalde gegevens noodzakelijk zijn voor de opsporing, dan is een algemene bewaarplicht noodzakelijk.

Het CBP constateert dat de feitelijke onderbouwing in het wetsontwerp van de noodzaak om deze gegevens van *de facto* elke Nederlander gedurende zes tot twaalf maanden te bewaren, tekort schiet. Zowel ten tijde van de invoering van de Wet bewaarplicht telecommunicatiegegevens[9], als nu bij de voorgestelde aanpassing ervan, gebruikt de regering voor de onderbouwing van de noodzaak van deze bewaarplicht kwalitatief onderzoek van respectievelijk de Erasmus Universiteit[10] en het WODC.[11] Deze rapporten geven de opvattingen weer van de ondervraagde experts uit de opsporingspraktijk, samengevat inhoudende dat de gegevens onmisbaar zijn voor de opsporing. Beide rapporten geven aan dat het niet mogelijk is om kwantitatief onderzoek te verrichten naar de relatie tussen het aantal opgevraagde historische telecommunicatiegegevens en de effectiviteit hiervan bij de bestrijding van ernstige misdrijven.[12]

---

[5] Hofarrest, paragraaf 51.

[6] Beleidsbrief Kabinet, p. 6.

[7] Idem, p. 10.

[8] Memorie van Toelichting, p. 10.

[9] De Wet bewaarplicht telecommunicatiegegevens is op 1 september 2009 in werking getreden.

[10] P. A.M. Mevis e.a., 'Wie wat bewaart heeft wat: Onderzoek naar nut en noodzaak van een bewaarverplichting van historische verkeersgegevens van telecommunicatie'. Erasmus Universiteit Rotterdam, 2005, URL: https://www.eerstekamer.nl/eu/behandeling/20050616/rapport_bijlage_bij_brief_5357934 (hierna: Mevis rapport).

[11] G. Odinot, D. de Jong, R.J. Bokhorst, C.J. de Poot, 'De Wet bewaarplicht telecommunicatiegegevens, Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing'. WODC 310, 2013, URL: https://www.wodc.nl/images/ob310-volledige-tekst_tcm44-534136.pdf (hierna: WODC rapport).

[12] WODC rapport, p. 29: "*Het is echter niet mogelijk om – zoals bij een product- of effectevaluatie het geval is – het effect vast te stellen van de invoering van de Wet bewaarplicht op de wijze waarop verkeersgegevens gebruikt worden in de opsporingspraktijk. Dit is niet goed mogelijk omdat de telecommunicatiegegevens waar het hier om draait ook vóór de*

Hoewel de bewaarplicht sinds 1 september 2009 in werking is getreden, en de opsporingsautoriteiten ruim vier en half jaar ervaring hebben opgedaan, is het kennelijk niet mogelijk gebleken een systematische onderbouwing te leveren van de noodzaak van deze bewaarplicht. Het CBP merkt tegelijkertijd op dat in Nederland veel gebruik wordt gemaakt van de bevoegdheid om bewaarde internet en telefoniegegevens op te vragen. In 2012 werden 56.825 vorderingen voor telecommunicatiegegevens gedaan door Justitie. Van dit totaal hadden volgens WODC 41.658 vorderingen betrekking op gegevens die in het kader van de bewaarplicht werden bewaard. Bijna de helft (42,6%) van deze vorderingen betrof gegevens die niet ouder waren dan drie maanden.[13] Ten aanzien van mastgegevens was zelfs 79% van de gevraagde gegevens niet ouder dan drie maanden.[14] De onderzoekers concluderen dat in driekwart van de gevallen de gevraagde gegevens niet ouder waren dan maximaal een half jaar.[15] Tegenover dit hoge aantal bevragingen staan 74 strafuitspraken van rechtbanken en hoven die de onderzoekers hebben gevonden waarin historische verkeersgegevens in dat jaar kenbaar een rol speelden.[16]

In dit overzicht van rechtszaken is geen nader onderscheid gemaakt tussen gegevens die beschikbaar zouden zijn geweest in de systemen van de telecomaanbieders zonder dat er een bewaarplicht was ingevoerd, of gegevens die bij aanvang van een onderzoek 'bevroren' hadden kunnen worden door de aanbieders, ten behoeve van later onderzoek. Uit het WODC-rapport blijkt dat het zwaartepunt van het opvragen van verkeersgegevens ligt bij het begin van het onderzoek.[17] Het wetsvoorstel bevat in het geheel geen uitwerking van de subsidiariteitstoets en onderbouwt niet waarom het alternatief van bevriezing van telecommunicatiegegevens, waarbij een relatie gelegd kan worden met ernstige criminaliteit, geen werkbaar alternatief oplevert ten

---

invoering van de Wet bewaarplicht in het algemeen beschikbaar waren voor de opsporing en gebruikt werden in de opsporingspraktijk." en Mevis rapport, p. 6: "*Het feit dat er uit de aangeboden selectie 65 zaaksdossiers zijn gevonden waarbinnen het gebruik van historische verkeersgegevens een (belangrijke) rol heeft gespeeld, kan niet leiden tot de wetenschappelijk onderbouwde conclusie dat die gegevens dus van (essentieel) belang zijn voor alle opsporingsonderzoeken. Uit de gehouden interviews kwam wel duidelijk naar voren dat men binnen de opsporing met grote regelmaat gebruik maakt van onderhavige bevoegdheid en dat veel voor de opsporing relevante informatie door middel van deze bevoegdheid verzameld wordt.*" In het Mevis rapport wordt ook de volgende conclusie getrokken: "*Wil men wetenschappelijk onderbouwde conclusies trekken over nut en noodzaak binnen de opsporingspraktijk van een bewaartermijn ruimer dan de nu gebruikelijke drie maanden, zou er zicht moeten zijn op het aantal strafrechtelijke onderzoeken die voordeel gehad zouden hebben bij een ruimere bewaartermijn en dus niet opgelost zijn of een langere doorlooptijd hebben gehad vanwege het niet meer aanwezig zijn van historische verkeersgegevens bij de aanbieders. In de aangeleverde opsporingsonderzoeken zijn dergelijke dossiers niet aangetroffen.*" Idem.

[13] WODC rapport, p. 120.

[14] WODC rapport, p. 121.

[15] WODC rapport, p. 87, tabel 6.1.1.

[16] Van de in totaal gepubliceerde en door het WODC geselecteerde 2.990 gepubliceerde strafuitspraken, kwamen historische verkeersgegevens voor in 74 uitspraken. WODC rapport, p. 128-129. Dit betreft dus minder dan een kwart procent van de gevallen. Ten aanzien van het gebruik van IP-adressen hebben de onderzoekers, zelfs met een langere zoekperiode van vier jaar, slechts 26 strafuitspraken gevonden. WODC rapport, p. 138.

[17] WODC rapport, p. 85.

opzichte van een algemene bewaarplicht. Een dergelijke specifieke bewaarplicht zou in zijn aard een geringere inbreuk maken op de rechten van alle Nederlanders.

Zonder afbreuk te willen doen aan de ernst van de voorbeelden die de regering in de Memorie van Toelichting geeft van het belang van het gebruik van historische telecommunicatiegegevens bij de opsporing van bepaalde vormen van ernstige criminaliteit, betreft het geen systematisch, met het gewicht van de voorgestelde maatregel overeenkomend, betoog over de noodzaak van de algemene bewaarplicht. De gegeven voorbeelden zijn, als het om het bewaren van internetverkeersgegevens gaat, eerder contrair aan het betoog dat een bewaartermijn van zes maanden noodzakelijk is voor de bestrijding van genoemde zeer ernstige misdrijven. In beide internetvoorbeelden gaat het over internetgegevens die pas na zes maanden of langer werden opgevraagd, en dus niet beschikbaar zouden zijn onder de bewaarplicht telecommunicatiegegevens.

Het CBP concludeert samenvattend dat het wetsontwerp geen adequate onderbouwing biedt van de noodzaak voor een algemene bewaarplicht voor internet en (internet)telefoniegegevens gedurende zes, respectievelijk twaalf maanden.

Ten aanzien van het noodzakelijkheidsvereiste wijst het CBP voorts op de jurisprudentie van het Europees Hof van de Rechten van de Mens (hierna: EHRM) ten aanzien van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM). Het EHRM heeft bij herhaling[18] gesteld dat een inperking van een grondrecht gerechtvaardigd kan zijn, wanneer dit in lijn is met nationale wetgeving, een rechtmatig doel wordt nagestreefd en de noodzaak in een democratische samenleving kan worden aangetoond. Er is echter geen vrijbrief voor landen om elke maatregel die passend wordt geacht ook in te voeren, aldus het EHRM in Klass/Duitsland: "*The Court, being aware of the danger such a law* [wetgeving die geheime surveillance mogelijk maakte, samenvatting CBP] *poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*"[19]

2.2 Proportionaliteit van een algemene bewaarplicht (van alle personen)

In het Hofarrest wordt veel aandacht besteed aan de proportionaliteitstoets, dat wil zeggen, de evenredigheid van het gekozen middel ten opzichte van het ermee te bereiken doel, in relatie tot de inbreuk die ermee wordt gemaakt op de grondrechten van burgers.

Het Hof stelt allereerst vast dat de dataretentierichtlijn van toepassing is "*op alle personen, alle elektronische communicatiemiddelen en alle telecommunicatiegegevens, zonder dat enig onderscheid wordt*

[18] Zie onder meer Leander/Zweden (EHRM, 26 maart 1987), paragrafen 49-67; K & T/Finland (EHRM, 12 juli 2001), paragrafen 151-155, S. en Marper/Verenigd Koninkrijk (EHRM, 4 december 2008), paragrafgen 95-104 en Khelili/Zwitserland (EHRM, 18 oktober 2011), paragrafen 58-71.

[19] Klass e.a./Bondsrepubliek Duitsland (EHRM 6 september 1978), paragraaf 49.

gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel, zware criminaliteit te bestrijden."[20] Ook stelt het Hof vast dat de richtlijn geen expliciete regeling biedt voor de toegang tot de gegevens. (Op dit punt voorziet het wetsvoorstel in een aanpassing.) Het Hof concludeert op basis van beide argumenten dat de dataretentierichtlijn "*geen duidelijke en precieze regels bevat betreffende de omvang van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten. Vastgesteld moet dus worden dat deze richtlijn een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke*."[21]

De analyse van het Hof komt in grote lijnen overeen met de kritiek die sinds de eerste voorstellen voor een bewaarplicht is geuit door de Europese toezichthouders voor gegevensbescherming, verenigd in de Artikel 29 Werkgroep. In een verklaring uit 2002, toen via de ePrivacy richtlijn de mogelijkheid van een nationale bewaarplicht telecommunicatiegegevens werd ingevoerd, schreven de toezichthouders: "*The European Data Protection Commissioners have grave doubt as to the legitimacy and legality of such broad measures.* (...) *The European Data Protection Commissioners have repeatedly emphasized that such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention of Human Rights* (…)."[22]

De Artikel 29 Werkgroep heeft deze beoordeling nadien verscheidene malen herhaald. In het najaar van 2005 stelde de Artikel 29 Werkgroep onder meer: "*A proportionate balance must be struck to ensure that we do not undermine the kind of society we are seeking to protect. This balance is especially necessary when forcing communication service providers to store data that they themselves have no need for. In this manner, one could eventually achieve the unprecedented, continued, pervasive monitoring of all kinds of communication and movement of the totality of citizens in their daily life. A huge amount of information would be stored that is actually useful for investigational purposes in a limited number of cases.*"[23]

De zorg over de proportionaliteit wordt in het Hofarrest als volgt verwoordt: : "*Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt (…) bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden.*"[24]

---

[20] Hofarrest, paragraaf 57-58.

[21] Hofarrest, paragraaf 65.

[22] Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 september 2002) on mandatory systematic retention of telecommunications traffic data, door het CBP bij brief van 2 september 2002 aangeboden aan de Minister van Justitie, CBP z2002-0885.

[23] Artikel 29-werkgroep, Opinie 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), 21 oktober 2005, p. 5.

[24] Hofarrest, paragraaf 37.

Het feit dat de bewaarplicht ziet op gegevens over het telecommunicatieverkeer, en niet op de inhoud van gesprekken, e-mails of websurfgedrag, maakt niet dat sprake is van een geringe inbreuk op het grondrecht bescherming persoonsgegevens. In 1984 heeft het EHRM al geoordeeld dat verkeersgegevens een integraal element vormen van de telecommunicatie, en dat het verstrekken van deze gegevens aan de politie een inbreuk vormt op het recht op privacy.[25]

De Artikel 29 Werkgroep schrijft hierover in zijn opinie naar aanleiding van de Snowden-onthullingen: "*It is also particularly important to note that metadata often yield information more easily than the actual contents of our communications do. They are easy to aggregate and analyse because of their structured nature. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours. This is not the case for the conversations, which can take place in any form or language. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours.*"[26]

Verkeersgegevens zijn daarom persoonsgegevens, die net zoveel bescherming behoeven als de inhoud van communicatie tussen personen.[27, 28, 29] Op grond van het wetsontwerp dienen de

---

[25] Malone/Verenigd Koninkrijk (EHRM, 2 augustus 1984), paragraaf 84. Het verwerken van verkeersgegevens *"is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts [...] to an interference with a right guaranteed by Article 8*."

[26] Artikel 29-Werkgroep, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 april 2014, p. 5. De Werkgroep onderbouwt dit standpunt onder meer met een verwijzing naar de schriftelijke verklaring die professor E.W. Felten heeft afgelegd ten overstaan van de United States District Court for the Southern District of New York in de zaak ACLU v. Clapper.

[27] Zie ook het rapport van de VN Hoge Commissaris voor de Mensenrechten, The right to privacy in the digital age, 30 juni 2014, URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/ Session27/ Documents/A.HRC.27.37_en.pdf, paragrafen 19-20: "*The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. As the European Union Court of Justice recently observed, communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained." (...) It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful* [onderstreping toegevoegd door het CBP]." En paragraaf 26: "*Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.*"

[28] Zie ook de mede door Nederland ingediende resolutie van 19 november 2014 van het Derde Comité van de Algemene Vergadering van de Verenigde Naties over The Right to Privacy in the Digital Age, URL:

telecommunicatieaanbieders deze gegevens van alle klanten te bewaren, ook de gegevens van klanten waarbij in het geheel geen aanwijzingen bestaat dat hun gedrag verband houdt met zware criminaliteit of dat er een verband bestaat met bedreiging van de openbare veiligheid.

In de beleidsbrief aan de Kamer schrijft de minister: "*Als de gegevens van deze personen niet bewaard mogen worden voordat het strafbare feit is gepleegd, zou het stellen van een dergelijke zoekvraag niet zinvol zijn. Het bewaren van bepaalde gegevens van alle burgers is derhalve noodzakelijk, nu niet op voorhand bij de opslag al kan worden onderscheiden tussen verdachte en niet-verdachte burgers.*"[30]

In deze beleidsbrief staat ook: "*Met het vereiste dat op basis van objectieve criteria per categorie gegevens duidelijk en precies wordt omschreven voor welke periode het strikt noodzakelijk is dat de gegevens door telecommunicatieaanbieders moeten worden bewaard, wordt voorbij gegaan aan de essentie van de bewaarplicht. Deze is dat bepaalde telecommunicatiegegevens beschikbaar moeten zijn voor de opsporing van ernstige misdrijven. Als de gegevens voor dat doel strikt noodzakelijk zijn, dan is bewaring daarvan aan de orde.*"[31]

Het feit dat de bewaarplicht niet wordt ingekaderd, en volgens de regering ook niet kán worden ingekaderd tot enkel die gegevens die noodzakelijk zijn om het beoogde doel te bereiken – de bestrijding van zware criminaliteit –, maakt dat de inbreuk op de artikelen 7 en 8 van het Handvest te groot is, en dat de maatregel niet voldoet aan het proportionaliteitsvereiste van artikel 8 EVRM. Naar het oordeel van het CBP kan hieruit worden afgeleid dat de voorgestelde instandhouding van een algemene bewaarplicht strijdig is met de in Europa geldende grondrechten, tenzij aan dit bewaren van de gegevens vooraf beperkingen kunnen worden gesteld.

Het CBP gaat in paragraaf 2.3 van dit advies nader in op het onderscheid dat de regering voorstelt tussen het bewaren van gegevens en de toegang ertoe, maar constateert hier reeds dat onder meer de conclusies van het Hof nopen tot heroverweging van het uitgangspunt van een algemene bewaarplicht voor telecommunicatiegegevens van *de facto* iedere Nederlander en daarmee van het gehele wetsontwerp.

Voor het CBP weegt het gebrek aan specifieke afbakening bij de evenredigheidstoets het zwaarst. Dit laat onverlet dat het wetsvoorstel, ook bij een eventueel nader afgebakende bewaarplicht, nog aan drie andere voorwaarden dient te voldoen om de proportionaliteitstoets te doorstaan. Dit zijn:

1. naleving van de notificatieplicht;

---

http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/69/L.26/Rev.1

"Noting that while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity."

[29] Zie ook CBP advies van 11 februari 2013 over het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet (z2012-00746) , p. 5-7.

[30] Beleidsbrief Kabinet, p. 8.

[31] Idem, p. 10.

2. controle op het gebruik van de bewaarde gegevens;
3. uitzonderingen voor mensen met een beroepsgeheim.

2.2.1 Naleving van de notificatieplicht
Het CBP leest in het Hofarrest een aanwijzing dat notificatie aan betrokkenen dat hun telecommunicatiegegevens zijn opgevraagd, een bijdrage levert aan de proportionaliteit van een maatregel om (specifieke) gegevens te bewaren ten behoeve van de opsporing. Zonder een deugdelijk notificatiesysteem kan bij iedereen in Nederland het gevoel ontstaan dat zij voortdurend bespied worden. Het Hof schrijft: "*Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of de geregistreerde gebruiker hierover wordt ingelicht, bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden, zoals de advocaat-generaal in de punten 52 en 72 van zijn conclusie heeft opgemerkt* [onderstreping toegevoegd door het CBP]."[32] Het CBP vraagt zich af hoe deze constatering van het Hof zich verhoudt tot de voorgenomen afschaffing van de notificatieplicht, zoals voorgesteld bij wetsontwerp van 30 september 2013.[33] Op 25 november 2013 heeft de vaste commissie voor Veiligheid en Justitie verslag uitgebracht; sindsdien heeft de minister niet meer gereageerd.

2.2.2 Controle op het gebruik van de bewaarde gegevens
In het gewijzigde artikel 13.9 van de Telecommunicatiewet is sprake van 'een verslag over de doeltreffendheid en de effecten van deze wet in de praktijk', dat elke drie jaar na de inwerkingtreding aan de Staten-Generaal wordt toegezonden. Van een horizonbepaling is geen sprake, evenmin als van een concrete invulling van de minimumvereisten waaraan een dergelijk verslag zou moeten voldoen.

Het CBP heeft kennis genomen van initiatieven van marktpartijen om anonieme en geaggregeerde statistieken openbaar te maken over aantallen intercepties en bevragingen van verkeers- en gebruikersgegevens. Hun doel is maatschappelijke transparantie te verschaffen over het gebruik van deze ingrijpende bevoegdheden door de overheid. De Minister van Veiligheid en Justitie heeft de telecom- en internetaanbieders, in beantwoording van Kamervragen hierover, ernstig ontraden om dergelijke statistieken openbaar te maken.[34] De minister verwijst daarbij naar een eerdere uitspraak van de staatssecretaris "*dat de verstrekking van geaggregeerde informatie de belangen van opsporing en vervolging ernstig in de weg kan staan. Een dergelijke verstrekking kan namelijk inzicht geven in de werkwijzen van de politie en het openbaar ministerie en kwaadwillenden zouden op basis hiervan hun werkwijze kunnen aanpassen*."

[32] Hofarrest, paragraaf 37.
[33] *Kamerstukken II*, 2013/14, 33 747, Wijziging van het Wetboek van Strafvordering en het Wetboek van Burgerlijke Rechtsvordering in verband met de versterking van het presterend vermogen van de politie.
[34] *Aanhangsel Handelingen*, 2013/14, 2014Z01266, 24 maart 2014.

De minister neemt in het jaaroverzicht van het ministerie van Veiligheid en Justitie een overzicht op van het totale aantal vorderingen 'historische gegevens' door het OM.[35] Dit jaarlijkse totaalaantal biedt echter geen inzage in de bevragingen door inlichtingen- en veiligheidsdiensten, en is bovendien moeilijk te interpreteren, omdat niet gespecificeerd is om hoeveel personen het gaat, over welke termijnen het gaat, en om wat voor soorten criminaliteit. WODC schrijft hierover: (...) *het opvragen van telecomgegevens in Nederland wordt geregistreerd per telefoonnummer, IMEI-nummer, IP-adres of 'paallocatie', waarover gegevens worden opgevraagd. Omdat mensen vaak meerdere telefoons gebruiken, geven deze cijfers geen inzicht in het aantal personen van wie er jaarlijks telecomgegevens worden opgevraagd of van het aantal opsporingsonderzoeken of de aard van de opsporingsonderzoeken waarvoor deze gegevens worden opgevraagd.*"[36] Ook bij het vorderen van mastgegevens gaat het om meer betrokken personen, omdat dan informatie wordt verkregen over alle mobiele gesprekken die op een bepaald tijdstip via een bepaalde mast zijn gevoerd. Bovendien betreffen de statistieken ook vorderingen van gegevens die niet onder de Wet bewaarplicht vallen.[37]

De stelling dat personen hun werkwijze zouden kunnen aanpassen op grond van anonieme, geaggregeerde statistieken, is niet onderbouwd. De regering gaat zonder toelichting voorbij aan het advies van het WODC om meer inzicht te bieden "*door de vorderingen zodanig te registreren dat zichtbaar wordt over hoeveel personen er jaarlijks telecommunicatieverkeersgegevens worden opgevraagd, in hoeveel zaken dit gebeurt en voor welke soort zaken deze gegevens worden opgevraagd.*"[38] Het ontbreken van transparantie op dit punt staat democratische controle op de (effectiviteit van de) uitoefening van bevoegdheden in de weg, en biedt ook geen inzicht aan burgers over de inzet van dit instrument.[39]

2.2.3 Uitzonderingen voor mensen met een beroepsgeheim

Aanvullend merkt het CBP op dat de voorgestelde wetsaanpassing niet tegemoet komt aan een ander kritiekpunt van het Hof, te weten dat de richtlijn geen uitzonderingen bevat voor de communicatie van mensen met een beroepsgeheim, zoals artsen, advocaten, notarissen of journalisten.[40]

---

[35] *Kamerstukken II*, 2013–2014, 33 930 VI, nr. 1, p. 50. Het meest recente jaarverslag bevat cijfers over 2013. In dat jaar zijn 62.554 ' aanvragen op historische gegevens' door het OM gedaan. Dit aantal omvat volgens de voetnoot zowel verkeersgegevens als identificerende gegevens.

[36] WODC rapport, p. 119.

[37] WODC rapport, p. 120.

[38] WODC rapport, p. 124.

[39] Het CBP wijst op het EHRM-arrest Youth Initiative For Human Rights/Servië (EHRM, 25 juni 2013), paragrafen 25-26. Ook de VN Hoge Commissaris voor de Mensenrechten merkt op: "*A second and related observation concerns the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability.*" (paragraaf 48).

[40] Hofarrest, paragraaf 58: "*Bovendien bevat de richtlijn geen uitzonderingen, zodat zij zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het zakengeheim vallen.*"

Samenvattend oordeelt het CBP dat de voorgestelde aanpassingen van de Wet bewaarplicht niet door de noodzakelijkheids-, proportionaliteits- en subsidiariteitstoets komen, en dat het wetsvoorstel op drie specifieke punten in strijd blijft met het proportionaliteitsvereiste, zoals vastgelegd in de artikelen 7 en 8 van het Handvest en in artikel 8 van het EVRM.

2.3 Verzamelen versus het gebruiken van gegevens

De regering stelt voor om een onderscheid te maken tussen het bewaren van de gegevens, en het gebruik ervan door de opsporings- en inlichtingendiensten en beschrijft dit in de beleidsbrief als een belangrijke waarborg om de inbreuk op de persoonlijke levenssfeer van betrokkenen te matigen. De regering stelt in de beleidsbrief dat de overwegingen van het Hof in samenhang dienen te worden bezien. De inbreuk die door de bewaarplicht telecommunicatiegegevens wordt gemaakt op de fundamentele rechten van burgers dient mede te worden vastgesteld aan de hand van de wettelijke waarborgen waarmee de bewaarplicht wordt omkleed. De regering meent zich in dit standpunt gesteund door overweging 69 van het arrest, waarin het Hof zijn conclusie trekt "gelet op een en ander" ("*having regard to all the foregoing considerations*"). Hieruit kan inderdaad opgemaakt worden dat de kritiek van het Hof in samenhang dient te worden bezien en dat het aanpassen van een onderdeel tot een andere conclusie zou kunnen leiden over het geheel.

Het CBP onderschrijft dat er een zekere samenhang bestaat tussen de mate van inbreuk en de voorziene waarborgen. Deze waarborgen dienen echter te gelden voor alle vormen van gegevensverwerking, waaronder in elk geval begrepen bewaren en het gebruik van de gegevens.

Het gaat hierbij niet om de gerichte opslag van gegevens van burgers die verdacht worden van misdrijven, maar om de ongerichte opslag van telecommunicatiegegevens over alle burgers. Of, zoals het Hof schrijft: (de richtlijn is van toepassing) "*op alle personen die gebruikmaken van elektronische communicatiediensten, zonder dat de personen van wie de gegevens worden bewaard zich echter, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met zware criminaliteit.*"[41]

Over de inbreuk die deze algemene bewaarplicht van persoonsgegevens vormt, schrijft de regering in de beleidsbrief: "*Ook de jurisprudentie van het EHRM geeft geen steun aan de opvatting dat een dergelijke gegevensopslag niet is toegestaan.*"[42] De zin is niet voorzien van een voetnoot met verwijzing naar de bedoelde jurisprudentie, en ook in de Memorie van Toelichting wordt hieraan geen aandacht besteed. In zijn arrest verwijst het Hof specifiek naar artikel 8 EVRM en de zaken Liberty e.a./Verenigd Koninkrijk, Rotaru/Roemenië, S. en Marper/Verenigd Koninkrijk en M. K./Frankrijk.[43]

---

[41] Hofarrest, paragraaf 58.

[42] Beleidsbrief Kabinet, p. 9.

[43] Hofarrest, paragrafen 47, 54 en 55.

In het S. en Marper/Verenigd Koninkrijk-arrest uit 2008 concludeerde het EHRM juist dat de opslag van (DNA- en vingerafdruk-)gegevens een inbreuk op de bescherming van de persoonlijke levenssfeer vormde, onafhankelijk van eventueel verder gebruik van die gegevens:

"*The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see Leander v. Sweden, 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (see Amann v. Switzerland [GC], no. 27798/95, § 69, ECHR 2000-II).*"[44]

In vergelijkbare woorden liet het Hof zich uit in het Liberty e.a./Verenigd Koninkrijk arrest:
"*The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (see Weber and Saravia, cited above, § 78).*"[45]

In het arrest Rotaru/Roemenië kwam het Hof acht jaar daarvoor al tot dezelfde conclusie: "*The Court points out that both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention (see the following judgments: Leander cited above, p. 22, § 48; Kopp v. Switzerland, 25 March 1998, Reports 1998-II, p. 540, § 53; and Amann cited above, §§ 69 and 80).*"[46]

In het meeste recente door het Hof geciteerde arrest, M. K./Frankrijk (2013), over de opslag van vingerafdrukken, geeft het Hof aan dat de toegang tot de bewaarde gegevens voldoende goed gedefinieerd en afgebakend is, maar dat dat van de verzameling en de opslag niet gezegd kan worden. Het Hof wijst het argument van de Franse regering dat de vingerafdrukken ook gebruikt kunnen worden om iemands onschuld te bewijzen in heldere bewoordingen af:
"*Besides the fact that such a reason is not explicitly mentioned in the provisions of Article 1 of the impugned decree, barring a particularly extensive interpretation of this Article, the Court considers that accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant*" [onderstreping toegevoegd door het CBP].[47]

Het CBP wijst in dit verband ook op de factsheet van het EHRM over de jurisprudentie met betrekking tot gegevensbescherming. De eerste alinea van dit overzicht is gewijd aan de vaststelling dat louter het opslaan van gegevens over iemands privéleven een inbreuk vormt op

[44] S. en Marper/Verenigd Koninkrijk (EHRM, 4 december 2008), paragraaf 67.
[45] Liberty e.a./Verenigd Koninkrijk (EHRM, 1 juli 2008), paragraaf 56.
[46] Rotaru/Roemenië (EHRM, 4 mei 2000), paragraaf 46.
[47] M. K./Frankrijk (EHRM, 18 april 2013), paragraaf 37.

artikel 8 EVRM.[48] De inbreuk wordt dus reeds gevormd door het enkele feit dat de gegevens worden opgeslagen (langer dan noodzakelijk voor de bedrijfsvoering) om te voldoen aan de wettelijk vereiste bewaarplicht.

Het CBP concludeert daarom dat het door de regering beoogde onderscheid tussen het bewaren van gegevens en het gebruik ervan, niet leidt tot beëindiging van de geconstateerde onevenredigheid en daarmee onrechtmatigheid van een algemene bewaarplicht verkeersgegevens. In zijn algemeenheid merkt het CBP in dit verband overigens op dat noch in internationale verdragen, noch in de Wet bescherming persoonsgegevens ruimte is te vinden voor het beoogde onderscheid tussen het bewaren van de persoonsgegevens en het gebruiken ervan, zoals het opvragen.

2.4 Overige voorgestelde aanpassingen

De regering komt met het wetsvoorstel tegemoet aan de kritiek van het Hof op het ontbreken van een voldoende afgebakende toegangsregeling in de richtlijn, met name op het ontbreken van het vereiste van onafhankelijke rechterlijke toetsing.[49] In het Wetboek van Strafvordering wordt voorzien in een voorafgaande schriftelijke machtiging door de rechter-commissaris van vorderingen door de officier van justitie. Deze aanpassing geeft het CBP geen aanleiding tot opmerkingen.

Ook komt het wetsvoorstel tegemoet aan de kritiek van het Hof dat de richtlijn niet verplicht stelt dat de gegevens op het grondgebied van de Unie worden bewaard, door aan de Telecommunicatiewet een expliciete verplichting toe te voegen om de gegevens in Nederland of in een andere lidstaat van de Europese Unie op te slaan en te verwerken.

Ten aanzien van het voorgestelde artikel 18.7, tweede lid, van de Telecommunicatiewet merkt het CBP op dat niet alleen het Agentschap Telecom toezicht houdt op het bepaalde bij of krachtens hoofdstuk 13, maar ook het CBP, voor zover het gaat om de verwerking van persoonsgegevens. De zinsnede in de Memorie van toelichting "*Andere toezichthouders (die aldus geen toezicht houden op de zogenoemde bewaarplicht) hebben geen toegang tot deze gegevens*"[50] lijkt het toezicht door het CBP uit te sluiten.

---

[48] EHRM, Press Unit, Factsheet - Data protection (september 2014), "*General Principles. Mere storage of information about an individual's private life amounts to interference within the meaning of Article 8 (right to respect for private life) of the European Convention on Human Rights.*" URL: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[49] Hofarrest, paragraaf 62: "*Maar bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten* (...)"

[50] Memorie van toelichting, p. 24.

Aanvullend merkt het CBP op dat in de richtlijn dataretentie, in artikel 9, tweede lid, was bepaald dat de toezichthoudende instanties "*volledig onafhankelijk zijn bij de uitoefening van de (...) bedoelde taak.*" Daarvan is in het Nederlandse voorstel geen sprake, nu deze taak is toebedeeld aan een agentschap onder directe verantwoordelijkheid van de minister van Economische Zaken. Het Hof benadrukt het belang van onafhankelijk toezicht, zoals vastgelegd in artikel 8, derde lid, van het Handvest. De bewaarde gegevens dienen volgens het Hof om die reden ook op het grondgebied van de Europese Unie te worden bewaard: "*zodat (...) ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest.*" De Memorie van Toelichting onderbouwt niet dat toebedeling van deze toezichtstaak aan een niet-onafhankelijke toezichthouder niet in strijd is met het Handvest en gaat ook niet in op de opmerking die de Raad van State hierover maakt: "*Ten volle moet zijn gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de beveiliging en bescherming van de opgeslagen gegevens.*"[51]

Ten aanzien van de wijzigingen van de lijst te bewaren gegevens merkt het CBP op dat het goed is dat een einde wordt gemaakt aan de onduidelijkheid bij marktpartijen over de omvang van de te bewaren locatiegegevens, nu expliciet is uitgesloten dat ook de locatie van de zendmast bij beëindiging van een gesprek moet worden vastgelegd (last Cell ID). Taalkundig lijken de voorgestelde aanpassingen overigens nog onvoldoende consistent doorgevoerd; er is onder punt B nog steeds sprake van telefonie, terwijl deze gegevens, conform het wetsontwerp, alleen nog op internettoegang zouden moeten zien.

Deze voorgestelde aanpassingen leiden niet tot een ander oordeel van het CBP over de noodzakelijkheid en proportionaliteit van de aangepaste Wet bewaarplicht telecommunicatiegegevens.

[51] Advies Raad van State, p. 11. De Raad van State schrijft ook: "(...)*zodat thans niet ten volle wordt gewaarborgd - zoals het Hof verlangt - dat het College bescherming persoonsgegevens toezicht kan houden op de beveiliging en bescherming van de opgeslagen gegevens.*" (p. 12).