Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directie Wetgeving en Juridische Zaken
Sector straf- en sanctierecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Ons kenmerk
586638

Uw kenmerk
2014Z0639/2014D13189

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

Datum 17 november 2014
Onderwerp Reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie

1. Inleiding en achtergrond

Op 8 april 2014 heeft het Hof van Justitie van de Europese Unie (hierna: Hof van Justitie) in de gevoegde zaken Digital Rights Ireland en Seitlinger uitspraak gedaan over de geldigheid van richtlijn 2006/24/EG (hierna: richtlijn dataretentie). Dit betreft de zaken C-293/12 en C294/12. De richtlijn dataretentie werd door het Hof van Justitie ongeldig verklaard.

Naar aanleiding van deze uitspraak heeft de staatssecretaris van Veiligheid en Justitie tijdens het mondelinge vragenuur, gehouden op 8 april 2014, aangegeven dat de Kamer na bestudering van de uitspraak zo snel mogelijk, naar verwachting binnen acht weken, gefundeerd zou worden geïnformeerd over de gevolgen van deze uitspraak voor de bewaarplicht voor telecommunicatiegegevens in Nederland (Handelingen Tweede Kamer 2013/2014, nr. 72, item 2, 8 april 2014).

Bij brief van 10 april 2014, kenmerk 2014Z06389/2014D13189, heeft de vaste commissie voor Veiligheid en Justitie mij om een reactie gevraagd op deze uitspraak van het Hof van Justitie en daarbij verzocht meer specifiek in te gaan op de volgende vragen:

- Welke (Nederlandse) wetten zijn op deze richtlijn gebaseerd? Wat betekent de uitspraak voor de bindendheid en uitvoering/uitwerking van deze wetten?
- Dient de Wet bewaarplicht telecommunicatiegegevens te worden aangepast?
- Zijn er effecten voor in Nederland opererende telecombedrijven en andere bedrijven waarop de Wet bewaarplicht telecommunicatiegegevens betrekking heeft? Zo ja, welke?
- Welke gevolgen heeft de uitspraak voor brede vormen van opslag van persoonsgegevens door de overheid die nu al bestaan en/of die de regering nog beoogt in te voeren?
- Wat zijn de gevolgen van de uitspraak voor de geheime diensten?

Bij brief van 23 april 2014, Kamerstukken I, 2013/14, 31 145, Y, heeft de vaste commissie voor Immigratie en Asiel / JBZ-Raad uitgesproken de bewaring en opslag van verkeers- en locatiegegevens overeenkomstig de richtlijn dataretentie een zeer omvangrijke en ernstige inmenging in fundamentele rechten te achten en de staatssecretaris van Veiligheid en Justitie gevraagd aan te geven welke

maatregelen dienaangaande getroffen zullen worden en op welke termijn de intrekking dan wel de schorsing van de bewaarplicht van verkeers- en locatiegegevens zal worden bewerkstelligd.

Tijdens het Algemeen Overleg over de verwerking en bescherming van persoonsgegevens, gehouden op 24 april 2014, hebben de vaste commissies voor Veiligheid en Justitie en voor Europese Zaken gevraagd over de uitspraak van het Hof van Justitie het advies van de Raad van State en van het College bescherming persoonsgegevens (Cbp) in te winnen. De staatssecretaris van Veiligheid en Justitie heeft in reactie daarop medegedeeld dat het dan niet uitgesloten is dat de reactietermijn van acht weken niet zou worden gehaald (Kamerstukken II 2013/14, 32 761, nr. 64, blz. 14-15 en 20). Tijdens het Algemeen Overleg over de JBZ-Raad, gehouden op 4 juni 2014, is door de staatssecretaris van Veiligheid en Justitie aangegeven dat enige vertraging is ontstaan en dat hij hoopte hierover begin juli meer duidelijkheid te kunnen geven (Kamerstukken II 2013/14, 32 317, nr. 246, blz. 19 en 23).

In deze brief wordt, namens het kabinet, ingegaan op de gevolgen van de uitspraak van het Hof van Justitie in de zaken Digital Rights Ireland en Seitlinger voor de bewaarplicht voor telecommunicatiegegevens en de naar aanleiding daarvan door Uw Kamer gestelde vragen.

Ten behoeve van een zorgvuldige oordeelsvorming heb ik, bij brief van 20 mei 2014, aan de Vicepresident van de Raad van State verzocht om mij op basis van artikel 21a, eerste lid, van de Wet op de Raad van State voorlichting te geven over de vraag welke mogelijke gevolgen dit arrest heeft voor de nationale wetgeving over de bewaring van telecommunicatiegegevens ten behoeve van de opsporing en vervolging van strafbare feiten. Bij brief van 17 juli 2014 heb ik de voorlichting van de Afdeling advisering van de Raad van State ontvangen. Bij het opstellen van de onderstaande reactie is met de voorlichting van de Raad van State rekening gehouden. Op basis van deze reactie is inmiddels een conceptwetsvoorstel opgesteld, dat voor advies aan het Cbp zal worden voorgelegd. Langs deze weg zal het advies van het Cbp worden ingewonnen over de consequenties van de uitspraak van het Hof van Justitie voor de bewaarplicht voor telecommunicatiegegevens in Nederland. Dit biedt de gelegenheid Uw Kamer thans te infomeren over de reactie van het kabinet naar aanleiding van de eerdergenoemde uitspraak van het Hof van Justitie en de voorlichting van de Afdeling advisering van de Raad van State openbaar te maken. De voorlichting is ter informatie bij deze brief gevoegd. Het conceptwetsvoorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische communicatiediensten is eveneens ter informatie bij deze brief gevoegd.

2. De richtlijn dataretentie

De richtlijn dataretentie had betrekking op de bewaring van telecommunicatiegegevens. De richtlijn had tot doel de nationale bepalingen van de lidstaten te harmoniseren waarbij aan de aanbieders verplichtingen werden opgelegd inzake het bewaren van bepaalde gegevens die door hen werden gegenereerd of verwerkt, teneinde te garanderen dat die gegevens beschikbaar waren voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit, zoals gedefinieerd in de nationale wetgevingen van de lidstaten. Het betrof hier zogenaamde verkeersgegevens: gegevens over het gebruik van telecommunicatie

door personen. De richtlijn dataretentie verplichtte de lidstaten ervoor te zorgen dat bepaalde categorieën van telecommunicatiegegevens werden bewaard voor een periode van ten minste zes maanden en ten hoogste twee jaar. De te bewaren categorieën van gegevens waren in de richtlijn opgesomd. Dit betrof gegevens over onder meer het nummer van oproeper en opgeroepene, tijd, duur van gesprek en locatie bij het begin van de verbinding. De inhoud van een gesprek of de inhoud van een sms-bericht viel niet onder de bewaarplicht. Historische verkeersgegevens van internet betroffen onder andere het e-mailadres van zender en ontvanger en de verkeersgegevens bij digitale telefonie. De inhoud van gesprekken, berichten of e-mails, zoektermen die zijn ingetypt in een zoekmachine en IP-adressen van bezochte internetpagina's vielen niet onder de richtlijn. De richtlijn dataretentie bepaalde dat de lidstaten bepalingen aannamen om te waarborgen dat de overeenkomstig deze richtlijn bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde autoriteiten werden verstrekt (artikel 4).

3. De Nederlandse wetgeving ter implementatie van de richtlijn dataretentie (geldend recht)

De richtlijn dataretentie is destijds in Nederland geïmplementeerd door middel van de Wet bewaarplicht telecommunicatiegegevens (Stb. 2009, 333), die met ingang van 1 september 2009 in werking is getreden, en de Wet van 6 juli 2011 tot wijziging van de Telecommunicatiewet in verband met de aanpassing van de bewaartermijn voor telecommunicatiegegevens met betrekking tot internettoegang, e-mail over het internet en internettelefonie (Stb. 2011, 350), die met ingang van 16 juli 2011 in werking is getreden. Tevens heeft de implementatie van de richtlijn dataretentie aanleiding gegeven tot aanpassing van het Besluit beveiliging gegevens telecommunicatie (Stb. 2009, 350).

De Wet bewaarplicht telecommunicatiegegevens voorziet in de aanvulling en wijziging van de hoofdstukken 11 (bescherming persoonsgegevens) en 13 (bevoegd aftappen) van de Telecommunicatiewet (Tw). Aanbieders van openbare telecommunicatienetwerken en -diensten bewaren gegevens, voor zover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. De bewaartermijn is twaalf maanden voor gegevens over telefonie, vanaf een vast of mobiel netwerk. Voor bepaalde vormen van internettelefonie, zoals Voice over IP (VoIP) hangen de functionaliteiten zo nauw samen met traditionele telefonie dat voor dergelijke diensten een bewaartermijn van twaalf maanden geldt. Voor internetgegevens (internettoegang, e-mail over het internet en andere vormen van internettelefonie) is de bewaartermijn zes maanden (artikel 13.2a, derde lid, Tw). De te bewaren gegevens zijn gelijk aan die van de Europese richtlijn. Naar aanleiding van de richtlijn is de bewaartermijn voor zogenoemde locatiegegevens verhoogd van drie naar twaalf maanden (artikel 13.4, derde lid, Tw). Dit ten behoeve van de bestandsanalyse om gegevens van zogenaamde prepaid kaarthouders te kunnen achterhalen (Besluit bijzondere vergaring nummergegevens).

Algemene strafvorderlijke bevoegdheden

De toegang tot de bewaarde gegevens wordt geregeld in het Wetboek van Strafvordering (en de Wet op de Inlichtingen en Veiligheidsdiensten 2002). Op grond van het Wetboek van Strafvordering is de officier van justitie bevoegd een

vordering te doen tot verstrekking van verkeersgegevens (artikel 126n/u Sv). Vereist is een verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. Naast de officier van justitie is de opsporingsambtenaar zelfstandig bevoegd een vordering te doen tot verstrekking van de zogenoemde gebruikersgegevens; dit betreft de gegevens inzake naam, adres, woonplaats, nummer en soort dienst. Dit betreft een veel beperktere categorie gegevens dan die welke op grond van de bevoegdheid tot het vorderen van verkeersgegevens kunnen worden verkregen. De toepassing van deze bevoegdheid is daarom niet beperkt tot de gevallen waarin sprake is van ernstige vormen van criminaliteit. Vereist is een verdenking van een misdrijf of een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd (artikel 126na/ua Sv).

Bijzondere bevoegdheden ter bestrijding van terrorisme
Tot slot hebben de officier van justitie en de opsporingsambtenaar specifieke bevoegdheden in verband met de bestrijding van terrorisme. De officier van justitie is, ingeval van aanwijzingen van een terroristisch misdrijf, bevoegd tot het vorderen van verkeersgegevens (artikel 126zh Sv). Naast de officier van justitie is de opsporingsambtenaar, ingeval van aanwijzingen van een terroristisch misdrijf, zelfstandig bevoegd tot het vorderen van gebruikersgegevens (artikel 126zi Sv).

Als een verkennend onderzoek de voorbereiding van de opsporing van terroristische misdrijven tot doel heeft, kan de officier van justitie in het belang van het onderzoek gegevensbestanden van publieke en particuliere instanties vorderen teneinde de hierin opgenomen gegevens te doen bewerken (artikel 126hh Sv). De gegevensbestanden kunnen worden doorzocht op bepaalde profielen en patronen van handelingen van personen die in het kader van de bestrijding van terrorisme van belang zijn. Hiervoor is een schriftelijke machtiging van de rechter-commissaris vereist. Dit betreft een algemene bevoegdheid die ook kan worden aangewend jegens aanbieders van telecommunicatiediensten of -netwerken.

De op grond van de Wet bewaarplicht telecommunicatiegegevens bewaarde gegevens vallen onder de Wet bescherming persoonsgegevens en hoofdstuk 11 van de Telecommunicatiewet. De persoonsgegevens die door de politie worden opgevraagd en vervolgens verder worden verwerkt ten behoeve van de opsporing van strafbare feiten, vallen onder de Wet politiegegevens. Het toezicht op de naleving van de regels wordt uitgeoefend door het Agentschap Telecom (AT) van het Ministerie van Economische Zaken en de Autoriteit Consument en Markt (ACM), in samenwerking met het Cbp.

De aanbieders zijn verplicht passende technische maatregelen te nemen om de bewaarde gegevens te beveiligen tegen onrechtmatig gebruik, te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen en dat de gegevens onverwijld worden vernietigd na afloop van de bewaartermijn (artikel 13.5, tweede en derde lid, Tw). In het Besluit beveiliging gegevens telecommunicatie zijn nadere regels gesteld over de beveiliging van de bewaarde gegevens. Dit betreft de verplichtingen tot het nemen van beveiligingsmaatregelen om kennisneming door onbevoegden te voorkomen, het opstellen van een beveiligingsplan, de screening van personen die toegang hebben tot de bewaarde gegevens en het vernietigen van de gegevens na afloop van de bewaartermijn.

4. De uitspraak van het Hof van Justitie van de Europese Unie

In het arrest van 8 april 2014 heeft het Hof van Justitie – op verzoek van het Ierse High Court en het Oostenrijkse Verfassungsgerichtshof - de geldigheid van de Europese richtlijn onderzocht in het bijzonder in het licht van twee door het Handvest van de grondrechten van de Europese Unie gewaarborgde grondrechten, te weten het recht op bescherming van het privéleven (artikel 7 van het Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 van het Handvest). Deze rechten bouwen voort op het recht op eerbiediging van privé-, familie- en gezinsleven van artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Het Hof van Justitie oordeelt dat de Europese richtlijn dataretentie met terugwerkende kracht ongeldig is. Daartoe overweegt het Hof van Justitie dat de te bewaren gegevens zeer nauwkeurige aanwijzingen kunnen verschaffen over het privéleven van degenen van wie de gegevens worden bewaard, zoals de gewoonten van het dagelijkse leven, de plaatsen van permanent of tijdelijk verblijf, de dagelijkse verplaatsingen, de sociale relaties en de gefrequenteerde sociale milieus. Het is niet ondenkbaar dat dit uiteindelijk raakt aan de vrijheid van meningsuiting ('freedom of speech'), die in artikel 11 van het Handvest is gegarandeerd (punt 28). De aantasting van die rechten door de richtlijn is vergaand en bijzonder ernstig (punt 37).

Op grond van het Handvest dient iedere beperking van de rechten en vrijheden van het Handvest bij wet te worden voorzien en, met inachtneming van het beginsel van proportionaliteit, zijn beperkingen op deze rechten en vrijheden uitsluitend mogelijk als deze noodzakelijk zijn en het doel van het algemeen belang dienen dat door de Unie is erkend (punt 38). Het beginsel van proportionaliteit vereist dat een EU-regeling passend ('appropriate') is om de gerechtvaardigde doelen van die regeling te realiseren en niet de grenzen van wat passend en noodzakelijk is overschrijdt. Volgens het Hof kan het bewaren van telecommunicatiegegevens worden beschouwd als passend om het doel van de richtlijn te bereiken (punt 49).

Het Hof van Justitie toetst vervolgens of de EU-regeling duidelijke en precieze regels betreffende de reikwijdte en de toepassing van de betrokken maatregel bevat, die minimale vereisten opleggen, zodat de betrokken personen over voldoende garanties beschikken dat hun persoonsgegevens worden beschermd tegen het risico van misbruik en onrechtmatig gebruik van de gegevens. Uit de toetsing van de verschillende bepalingen van de richtlijn dataretentie volgt volgens het Hof van Justitie dat de richtlijn dataretentie geen duidelijke en precieze regels stelt over de mate van aantasting van de fundamentele rechten van het Handvest voor de grondrechten (punt 65). Gelet op één en ander moet worden geoordeeld dat de wetgever van de Unie met de vaststelling van de richtlijn dataretentie de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, eerste lid van het Handvest in acht dient te nemen (punt 69). Op de aan dit oordeel ten grondslag liggende overwegingen wordt hieronder, bij de bespreking van de reactie van het kabinet op de gevolgen van dit arrest voor de nationale wetgeving, nader in gegaan. De Europese Commissie heeft de mogelijkheid om een nieuwe richtlijn voor te stellen aangehouden tot na de formatie van de nieuwe Commissie. Het is thans niet zeker of de nieuwe Europese Commissaris hiertoe een initiatief zal nemen.

5. De gevolgen van het arrest voor de Nederlandse wetgeving op het gebied van de bewaarplicht voor telecommunicatiegegevens

De precieze duiding van de mogelijke gevolgen van het arrest van het Hof van Justitie voor de Nederlandse wetgeving op het gebied van de bewaarplicht voor telecommunicatiegegevens vergt een zorgvuldige analyse. Het Hof van Justitie stelt allereerst vast dat het bewaren van telecommunicatiegegevens ten behoeve van het voorkomen van strafbare feiten en het bestrijden van criminaliteit daadwerkelijk aan een doel van algemeen belang beantwoordt (punt 44). Gelet op het toenemende belang van elektronische communicatiemiddelen biedt het bewaren van deze gegevens de autoriteiten een waardevol instrument bij strafonderzoeken. De bewaring van dergelijke gegevens is derhalve geschikt voor het door deze richtlijn nagestreefde doel (punt 49). Vervolgens overweegt het Hof van Justitie dat de regeling niet voldoende precieze en duidelijke regels stelt over de reikwijdte en toepassing van de betrokken maatregel die minimale vereisten opleggen, zodat de betrokken personen worden beschermd tegen het risico van misbruik of onrechtmatig gebruik van de gegevens (punt 54). Het Hof van Justitie stelt vast dat de richtlijn een zeer ruime en bijzonder zware inmenging in de door de artikelen 7 en 8 van het Handvest van de grondrechten erkende fundamentele rechten bevat, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke (punt 65).

Hieronder wordt nader ingegaan op de gevolgen van het arrest van het Hof van Justitie en de naar aanleiding van die uitspraak door de leden van Uw Kamer gestelde vragen.

5.1. Kan de Nederlandse wetgeving op het gebied van de bewaring van telecommunicatiegegevens in stand blijven ?

Allereerst is de vraag aan de orde of de Wet bewaarplicht telecommunicatiegegevens in stand kan blijven, nu de richtlijn dataretentie ongeldig is verklaard. De regering beantwoordt die vraag bevestigend. De Nederlandse wetgeving is rechtsgeldig tot stand gekomen, op basis van de daarvoor geldende procedures. Ook de Afdeling advisering concludeert dat het enkele feit dat het Hof van Justitie de richtlijn dataretentie ongeldig heeft verklaard, niet betekent dat de nationale wetgeving ter omzetting van die richtlijn daardoor ongeldig wordt. De Nederlandse wetgever heeft een algemene bevoegdheid om regels te stellen. De Nederlandse wetgeving bevat reeds waarborgen die verder gaan dan die van de richtlijn dataretentie, zoals de regels in het Wetboek van Strafvordering over de toegang tot de bewaarde gegevens. Wel zal die tot stand gekomen wetgeving in overeenstemming moeten zijn of worden gebracht met de (nieuwe) uitleg van de bestaande grondrechten die strekken tot bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens. Dit komt hieronder nader aan de orde.

5.2. Is een bewaarplicht voor telecommunicatiegegevens noodzakelijk?

De regering is overtuigd 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. Ook op grond van de

bestaande bevoegdheden in het Wetboek van Strafvordering kunnen gegevens worden gevorderd van de aanbieders van telecommunicatiediensten, maar zonder een wettelijke bewaarplicht is het niet bij voorbaat zeker dat die gegevens bij de aanbieders beschikbaar zijn. De snelle technische ontwikkelingen binnen de communicatietechnologie maken het onzeker of de gegevens, die voor de opsporing en vervolging van belang zijn, door de aanbieders worden verwerkt ten behoeve van hun eigen bedrijfsvoering en dus ook voor de opsporing en vervolging beschikbaar zijn. Naast de bewaarplicht als zodanig is de concrete bewaartermijn van groot belang, omdat de duur van de bewaartermijn direct van invloed is op de beschikbaarheid van de gegevens voor de opsporing en vervolging. Juist in een later stadium kan blijken dat bepaalde telecommunicatiegegevens van belang zijn voor een opsporingsonderzoek, zonder dat op het moment van de vastlegging van de gegevens sprake was van inzicht in de betrokkenheid van de personen bij ernstige misdrijven. Hiervan kunnen talloze voorbeelden worden gegeven. Eén daarvan betrof een medepleger van twee gewelddadige roofovervallen in Rotterdam, waarbij een medepleger tien maanden na de pleegdatum in beeld kwam. Een ander geval betrof een verkrachting waarbij het langlopende onderzoek uiteindelijk tot de dader leidde, mede dankzij verkeersgegevens waarmee kon worden aangetoond dat de verdachte toentertijd bij het slachtoffer in de buurt was geweest. Weer een ander geval betrof een internationaal onderzoek naar kindermisbruik, waarbij kinderen jonger dan tien jaar zeer ernstig werden misbruikt. Tot de IP-adressen behoorden die van meer dan honderd Nederlanders. Geen van deze zaken kon echter in behandeling worden genomen omdat de bewaartermijn verstreken was, waardoor het IP-adres niet meer aan een gebruiker kon worden gekoppeld. Hiervoor kan ook worden verwezen naar de publicatie van de Europese Unie over de noodzaak voor dataretentie in de Europese Unie[1].

5.3. Dient de Nederlandse wetgeving op het gebied van de bewaring van telecommunicatiegegevens te worden aangepast?

Vervolgens is de vraag aan de orde of de Wet bewaarplicht telecommunicatiegegevens aangepast moet worden, in het licht van de uitspraak van het Hof van Justitie. De regering beantwoordt deze vraag eveneens bevestigend. Nationale regels over de bewaring van telecommunicatiegegevens zijn relevant voor het vrije verkeer van diensten binnen de Europese Unie en vallen, nu de richtlijn dataretentie ongeldig is verklaard, onder de reikwijdte van richtlijn 2002/58/EG (e-privacyrichtlijn). Op grond van deze richtlijn kunnen de lidstaten regels stellen voor het bewaren van telecommunicatiegegevens, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van legitieme belangen, waaronder het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Daartoe kunnen lidstaten onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode voor die doelen te bewaren. Deze maatregelen dienen in overeenstemming te zijn met het gemeenschapsrecht, met inbegrip van de beginselen, bedoeld in het Handvest van de grondrechten en het EVRM. Omdat een dergelijke bewaarplicht binnen de werkingssfeer van de e-privacyrichtlijn valt (artikel 15, eerste lid, e-privacyrichtlijn) en dus binnen de werkingssfeer van het recht van de Europese Unie, valt deze tevens onder de werkingssfeer van het Handvest van de grondrechten.

[1] http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf.

De Afdeling advisering stelt vast dat de Wet bewaarplicht telecommunicatiegegevens de door het Hof van Justitie gewraakte bepalingen van de richtlijn dataretentie omzet en dat toetsing van de Wet bewaarplicht telecommunicatiegegevens aan het Handvest van de grondrechten tot de conclusie leidt dat deze wet, net als de richtlijn dataretentie, in strijd is met de artikelen 7 en 8 van het Handvest van de grondrechten. Hieruit vloeit voort dat de nationale wetgeving moet worden aangepast voor zover deze niet in overeenstemming is met het Handvest van de grondrechten. De Nederlandse regering kan deze zienswijze onderschrijven. Hieronder zal ik nader ingaan op de diverse eisen die het Hof van Justitie heeft gesteld aan de opslag van (telecommunicatie)gegevens en daarbij aangeven op welke punten de Wet bewaarplicht telecommunicatiegegevens aanpassing behoeft om te voldoen aan het Handvest van de grondrechten.

5.3.1. Eisen aan de wetgeving

Het Hof van Justitie overweegt dat met het bewaren van de gegevens een legitiem doel wordt nagestreefd, namelijk de bestrijding van ernstige criminaliteit (punt 44 en 51). Dit, op zichzelf, maakt evenwel nog niet dat de regeling in overeenstemming is met het Handvest van de grondrechten. De bewaarplicht moet, aldus het Hof van Justitie, beperkt zijn tot wat strikt noodzakelijk is (punt 52) en er moeten duidelijke en precieze regels worden gesteld. Vervolgens wordt overwogen dat de richtlijn dataretentie algemeen van toepassing is op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld, of enige uitzondering wordt gemaakt op basis van het doel, criminaliteit te bestrijden (punt 57). Het Hof van Justitie overweegt daarbij dat de richtlijn dataretentie zelfs van toepassing is op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag een verband vertoont met zware criminaliteit (punt 58).

De Afdeling advisering leidt uit deze overwegingen van het Hof van Justitie af dat een Europese regeling duidelijk en precies moet omschrijven welke categorieën gegevens, van welke historische communicatiemiddelen, van welke personen strikt noodzakelijk zijn voor het voorkomen, opsporen of vervolgen van criminaliteit en dus door telecommunicatieaanbieders moeten worden opgeslagen. Daarbij moeten er aanwijzingen bestaan dat er een verband bestaat tussen het gedrag van de personen van wie gegevens worden opgeslagen en zware criminaliteit.
Naar aanleiding hiervan merk ik op dat de wettelijke bewaarplicht ertoe dient te verzekeren dat historische telecommunicatiegegevens beschikbaar zijn, als achteraf blijkt van de relevantie van die gegevens voor opsporing en vervolging. Als een strafbaar feit wordt gepleegd kan het van belang zijn te achterhalen met wie het slachtoffer of een verdachte voorafgaand aan het strafbare feit contact heeft gehad, zodat de daders respectievelijk de mededaders in beeld kunnen worden gebracht. 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. De bewaring 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. Anders dan de Afdeling advisering is de regering van oordeel dat de desbetreffende overwegingen van het Hof van Justitie in hun onderlinge samenhang dienen te worden bezien. Zou het inzicht van de Afdeling advisering, dat aan elke door het

Hof van Justitie genoemde waarborg afzonderlijk moet worden voldaan, juist zijn, dan zou reeds het enkele feit dat gegevens van burgers worden bewaard, zonder dat er op het moment van de opslag sprake is van aanwijzingen dat hun gedrag een verband vertoont met zware criminaliteit, voldoende zijn voor de ongeldigverklaring van de richtlijn dataretentie. Het Hof van Justitie oordeelt echter dat gelet op alle overwegingen ('Gelet op één en ander, ofwel: 'Having regard to all the foregoing considerations') de wetgever van de Unie met de vaststelling van de richtlijn dataretentie de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, eerste lid, van het Handvest van de g
rondrechten in acht had dienen te nemen (punt 69). Ook de jurisprudentie van het EHRM geeft geen steun aan de opvatting dat een dergelijke gegevensopslag niet is toegestaan. In het licht hiervan dient de desbetreffende overweging van het Hof van Justitie naar het oordeel van de regering zo te worden uitgelegd, dat het feit dat de richtlijn geen enkel verband vereist tussen de opslag van gegevens en het gedrag van personen, weliswaar een zeer vergaande inbreuk op de persoonlijke levenssfeer van de betrokkenen kan vormen, maar dat de ernst van die inbreuk kan worden gematigd door het opnemen van passende garanties en waarborgen voor een zorgvuldige wijze van bewaren en verwerken van gegevens, alsmede de toegang tot die gegevens. De vereiste matiging kan worden bereikt door enkele elkaar versterkende aanpassingen in de wet aan te brengen. De door het Hof van Justitie geconstateerde mate van inbreuk op de persoonlijke levenssfeer noopt ertoe de aard en omvang van de bewaarplicht op grond van de Nederlandse Wet bewaarplicht telecommunicatiegegevens, evenals de daarbij geldende waarborgen en garanties, zeer kritisch te onderzoeken. Op deze aspecten wordt hieronder nader ingegaan. Achtereenvolgens zal worden stilgestaan bij de vraag in hoeverre de bewaartermijnen en de categorieën van te bewaren gegevens moeten worden aangepast en of de regels met betrekking tot de toegang tot de gegevens en de bescherming en beveiliging aanpassing behoeven.

5.3.2. De bewaartermijnen en de categorieën van te bewaren gegevens

Het Hof van Justitie overweegt dat in de richtlijn dataretentie, met een bewaartermijn van ten minste zes maanden, geen onderscheid wordt gemaakt in de categorieën van gegevens en hun mogelijke betekenis voor het nagestreefde doel (punt 63). Verder is in de richtlijn niet bepaald dat de vaststelling van de bewaartermijn – die tussen de zes en vierentwintig maanden moet zijn - gebaseerd moet zijn op objectieve criteria, zodat gewaarborgd is dat deze is beperkt tot wat strikt noodzakelijk is (punt 64).
De Afdeling advisering merkt op dat het Hof van Justitie verlangt dat er bij de bewaartermijn onderscheid wordt gemaakt tussen de verschillende categorieën gegevens naar gelang van het nut voor het nagestreefde doel en naargelang van de betrokken personen, en dat de bewaartermijn wordt vastgesteld op basis van objectieve criteria voor de verschillende soorten van gegevens die moeten worden bewaard. Een dergelijk onderscheid ontbreekt in de Wet bewaarplicht telecommunicatiegegevens, waarin slechts onderscheid wordt gemaakt tussen gegevens over telefonie en gegevens over internet, e-mail en internettelefonie.

Naar aanleiding hiervan zijn de bewaartermijnen voor telecommunicatiegegevens heroverwogen. Daarbij is rekening gehouden met de kaders van artikel 15, eerste lid, van de e-privacyrichtlijn. Immers, nu de richtlijn dataretentie ongeldig is verklaard kan een nationale bewaarplicht voor telecommunicatiegegevens slechts

worden vastgesteld binnen de grenzen van die richtlijn. In de e-privacyrichtlijn is niet aangegeven wat precies dient te worden verstaan onder een beperkte periode, als bedoeld in artikel 15, eerste lid, van die richtlijn. De maatregelen dienen passend te zijn voor, en strikt noodzakelijk in een democratische samenleving en moeten adequate waarborgen bevatten overeenkomstig het EVRM (Preambule bij de e-privacyrichtlijn, punt 11). Dit impliceert wijziging van de artikelen 13.2a, derde lid en 13.4, derde lid van de Telecommunicatiewet.

Bij het bepalen van de bewaartermijn dienen zowel de privacyaspecten als de noodzakelijkheid voor de opsporing te worden betrokken. Met inachtneming daarvan acht de regering het aangewezen de bewaartermijnen onveranderd te laten. Dat wil zeggen, een bewaartermijn van zes maanden voor internetgegevens en twaalf maanden voor telefoniegegevens. Om de aantasting van de persoonlijke levenssfeer in verband met de bewaring van telecommunicatiegegevens zoveel mogelijk te beperken wordt voorgesteld de regels met betrekking tot de toegang tot de gegevens en de bescherming en beveiliging aan te passen. Hierop wordt hieronder nader ingegaan.

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 voorbijgegaan 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. Als de gegevens voor dat doel niet strikt noodzakelijk zijn, dan is dit niet het geval. Het maken van onderscheid in de categorieën van gegevens is hiermee niet verenigbaar. Aan dit vereiste kan wel langs andere weg worden vormgegeven. Onderscheid kan worden gemaakt in de periode van beschikbaarheid van de gegevens voor de opsporing van ernstige misdrijven, in die zin dat de duur van de toegang toeneemt afhankelijk van de ernst van het betreffende misdrijf. Aldus kan aan de hand van een objectief criterium, namelijk de ernst van het betreffende strafbare feit, nadere differentiatie worden aangebracht in de beschikbaarheid van de gegevens ten behoeve van de criminaliteitsbestrijding. Dit impliceert wijziging van de artikelen 126n/u van het Wetboek van Strafvordering.

5.3.3. De toegang tot de bewaarde gegevens

Het Hof van Justitie overweegt dat de richtlijn geen objectief criterium bevat dat de toegang van de bevoegde autoriteiten tot de gegevens beperkt. In de richtlijn wordt verwezen naar ernstige criminaliteit, zoals door de lidstaten in hun nationale wetgeving gedefinieerd (punt 60). Verder bevat de richtlijn geen inhoudelijke en procedurele voorwaarden voor de toegang van de bevoegde autoriteiten tot de gegevens en hun verdere gebruik. Nadere regeling daarvan wordt overgelaten aan de lidstaten (punt 61). In het bijzonder bevat de richtlijn geen objectief criterium ter beperking van het aantal personen dat wordt geautoriseerd voor de toegang, en het verdere gebruik van de gegevens, tot hetgeen strikt noodzakelijk is in het licht van de te bereiken doelen. Bovenal is de toegang van de bevoegde autoriteiten tot de bewaarde gegevens niet afhankelijk gesteld van voorafgaande toetsing door een gerecht of een onafhankelijk bestuurlijk orgaan naar aanleiding van een gemotiveerd verzoek van de aangewezen autoriteiten (punt 62).

Rechtstreekse toegang tot de database is in Nederland al streng gereguleerd. Uitsluitend geautoriseerde medewerkers van de providers hebben toegang tot de bewaarde gegevens. De beschikbaarstelling van gegevens door de aanbieders van openbare telecommunicatienetwerken en -diensten ten behoeve van de opsporing en vervolging van strafbare feiten wordt beheerst door de regels van het Wetboek van Strafvordering. Op grond van die regels kan de officier van justitie, in geval van een verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of ingeval van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, in het belang van het onderzoek een vordering doen tot verstrekking van verkeersgegevens. In artikel 67, eerste lid, van het Wetboek van Strafvordering zijn de misdrijven opgesomd waarvoor voorlopige hechtenis mogelijk is. Aldus is de toegang tot de bewaarde verkeersgegevens ten behoeve van de opsporing en vervolging van strafbare feiten in de Nederlandse wetgeving – anders dan in de richtlijn dataretentie - beperkt tot gevallen waarin sprake is van ernstige misdrijven.

Naar aanleiding van het arrest van het Hof van Justitie is de regering voornemens extra waarborgen te treffen met het oog op verdere matiging van de toegang tot de bewaarde gegevens. In de eerste plaats door de introductie van een systeem van differentiatie in de toegang tot de gegevens en tevens door de introductie van een voorafgaande rechterlijke toetsing.

Het systeem van differentiatie strekt er toe dat de volledige bewaartermijn, anders dan tot nu toe, alleen volledig wordt benut wanneer sprake is van de zwaarste categorie delicten waarop zeer lange vrijheidsstraffen zijn gesteld. Bij lichtere delicten, waarvoor weliswaar voorlopige hechtenis kan worden opgelegd maar waarvoor geen zeer lange strafdreiging geldt, kunnen de gegevens gedurende een kortere periode worden gevorderd. In die laatste situatie kunnen de gegevens wel onder de bewaarplicht vallen, maar kan de officier van justitie de gegevens niet vorderen ten behoeve van de opsporing van een bepaald misdrijf omdat dit niet van voldoende ernst is om de toegang tot de gegevens te rechtvaardigen.

Aanvullend wordt een rechterlijke toetsing voorgesteld. Thans is, zoals gezegd, de bevoegdheid tot het vorderen van verkeersgegevens voorbehouden aan de officier van justitie. Door de toegang tot de bewaarde gegevens afhankelijk te stellen van een voorafgaande rechterlijke toetsing wordt nog meer gewaarborgd dat de gegevens slechts worden geraadpleegd in de gevallen waarin daartoe voldoende aanleiding bestaat en dat de privacy van burgers afdoende wordt beschermd. Daartoe zal in het Wetboek van Strafvordering worden geregeld dat de vordering van de bewaarde gegevens afhankelijk is van een voorafgaande machtiging van de rechter-commissaris.

Daarnaast geldt dat de opsporingsambtenaar, ingeval van een verdenking van een misdrijf of ingeval van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, in het belang van het onderzoek historische gebruikersgegevens kan vorderen (art. 126na/ua Sv). Een soortgelijke bevoegdheid geldt ingeval van aanwijzingen van een terroristisch misdrijf (art. 126zi Sv). Het betreft hier gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst. Onder «soort dienst» wordt verstaan het type

telecommunicatiedienst dat de gebruiker van de aanbieder afneemt, zoals vaste of mobiele telefonie, internet of om soorten binnen deze diensten, zoals telefax. De toepassing van deze bevoegdheden is mogelijk in geval van verdenking van een misdrijf, en is niet beperkt tot de gevallen waarin sprake is van verdenking van een ernstig misdrijf.

De regering is van oordeel dat de categorie van de gebruikersgegevens, zoals reeds eerder opgemerkt, een veel beperktere categorie van gegevens betreft. Uit deze gegevens kunnen geen precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals dat naar het oordeel van het Hof van Justitie aan de orde is bij de bewaring van de verkeersgegevens op grond van de richtlijn dataretentie (punt 27). Naar het oordeel van de regering dient het bewaren van de gebruikersgegevens dan ook anders te worden gewaardeerd dan het bewaren van de verkeersgegevens, en behoeft de huidige wettelijke regeling op dit punt geen aanpassing.

5.3.4. De bescherming en beveiliging van de gegevens

Het Hof van Justitie overweegt tenslotte dat de richtlijn dataretentie bovendien niet voorziet in afdoende waarborgen voor een effectieve bescherming tegen het risico van misbruik en tegen onrechtmatige raadpleging van de gegevens. De richtlijn bevat geen specifieke regels die aangepast zijn aan de enorme hoeveelheid gegevens die bewaard moeten worden, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd. Er is ook geen verplichting voor de lidstaten om in dergelijke regels te voorzien (punt 66). De richtlijn waarborgt niet dat de aanbieders via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden, maar biedt de aanbieders de mogelijkheid om hierbij rekening te houden met economische overwegingen. In het bijzonder waarborgt de richtlijn niet dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd (punt 67). Ook schrijft de richtlijn dataretentie niet voor dat de betrokken gegevens op het grondgebied van de Unie worden bewaard, zodat niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk voorgeschreven door artikel 8, derde lid, van het Handvest van de Grondrechten (punt 68).

Naar aanleiding van deze overwegingen merkt de regering op dat in de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet reeds waarborgen en voorschriften zijn opgenomen, op grond waarvan de aanbieders passende technische en organisatorische maatregelen dienen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (artikelen 13 Wbp en 11.3 Tw). Deze normen vormen de implementatie van Europese regels. Hierbij kunnen de aanbieders weliswaar rekening houden met de stand van de techniek en de kosten van de tenuitvoerlegging maar voorop staat dat de maatregelen passend zijn, gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. Hieruit vloeit voort dat de veiligheid en beveiliging van de aangeboden netwerken en diensten te allen tijde gewaarborgd moeten zijn. Het College bescherming persoonsgegevens ziet toe op de naleving van artikel 13 Wbp en artikel 11.3 Tw. Naast het Cbp is ook de ACM belast met toezicht op artikel 11.3 Tw. In aanvulling op die verplichtingen zijn de aanbieders gehouden passende technische en organisatorische maatregelen te treffen teneinde de

gegevens te beveiligen tegen vernietiging, verlies of wijziging en niet toegelaten opslag, verwerking, toegang of openbaarmaking, te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen, en de gegevens te kunnen vernietigen na afloop van de bewaartermijn (art. 13.5, tweede lid, Tw). Daarbij wordt de aanbieders geen ruimte gelaten om rekening te houden met economische overwegingen. Voorts zijn in het Besluit beveiliging gegevens telecommunicatie regels opgenomen voor de beveiliging van de toegang tot de bewaarde gegevens. Bovendien voorziet de Telecommunicatiewet, zoals ook de Afdeling advisering heeft opgemerkt, in een verplichting tot onverwijlde vernietiging van de gegevens (artikel 13.5, derde lid, Tw). Agentschap Telecom (AT) ziet toe op de naleving van artikel 13.5 Tw. Bij brief van 16 mei 2014 heeft de Minister van Economische Zaken het rapport "Meting dataretentie 2013"aan Uw Kamer aangeboden (Kamerstukken II 2013/14, 26 643, nr. 313). Dit rapport beoogt inzicht te bieden in de naleving van de Wet bewaarplicht telecommunicatiegegevens. Uit de periodieke en individuele controles van de aanbieders blijkt dat zij over het algemeen voldoen aan de wettelijke voorschriften op het gebied van het bewaren van gegevens en privacy van hun klanten. In het licht van de wettelijke regels en de ervaringen daarmee in de praktijk is de regering van oordeel dat de Nederlandse regeling in zijn algemeenheid voldoet aan de door het Hof van Justitie gestelde eisen op het gebied van de bescherming en de beveiliging van de bewaarde gegevens. Op enkele onderdelen acht de regering echter aanpassing noodzakelijk.

Nadere regels over de beveiliging van de bewaarde gegevens zijn opgenomen in het Besluit beveiliging gegevens telecommunicatie. De bewaarde gegevens mogen slechts voor een beperkt aantal medewerkers van de aanbieder toegankelijk zijn. Gezien de gevoeligheid van deze gegevens ligt het in de rede om de gegevens die ten behoeve van de opsporing en vervolging worden bewaard, volledig af te schermen tegen inzage door onbevoegden. De regering zal onderzoeken of versleuteling van deze gegevens kan plaatsvinden.

De Afdeling advisering heeft erop gewezen dat het Nederlandse recht, net als de richtlijn dataretentie, geen verplichting bevat de gegevens op het grondgebied van de Unie te bewaren, zodat thans niet ten volle is gewaarborgd – zoals het Hof verlangt – dat het Cbp toezicht kan houden op de beveiliging en bescherming van de opgeslagen gegevens. Het Hof van Justitie legt daarbij uitdrukkelijk een verband met het doel daarvan: het verzekeren dat de gegevens voldoende beveiligd en beschermd zijn. In reactie hierop is de regering voornemens de regeling in de Telecommunicatiewet aan te passen, zodat de aanbieders worden verplicht de te bewaren gegevens binnen de Europese Unie op te slaan en te verwerken. Het toezicht op de naleving van de normen op het gebied van de bescherming en beveiliging van de bewaarde gegevens, die voor een belangrijk deel voortvloeien uit Europese regels, kan daarmee worden verbeterd.

Het toezicht op de naleving van hoofdstuk 13 van de Telecommunicatiewet is in handen van de Minister van Economische Zaken en het CBP. De Minister maakt daarvoor gebruik van de ambtenaren van Agentschap Telecom. De toezichthoudende taak van de Minister van Economische Zaken doet op geen enkele wijze afbreuk aan de toezichtbevoegdheden die het Cbp heeft met betrekking tot het gebruik van gegevens die zijn aan te merken als persoonsgegevens. Het toezicht van AT is thans ingericht als systeemtoezicht. Dit wil zeggen dat AT de bedrijfsvoeringsprocessen en de borging hiervan beoordeelt. Op grond van de regeling van de Telecommunicatiewet is AT echter niet bevoegd

om de verkeersgegevens op te vragen die door aanbieders op grond van de wettelijke bewaarplicht moeten worden bewaard. Hiermee mist het AT een nuttig instrument om dit aspect van het toezicht uit te kunnen voeren. De regering is voornemens de Telecommunicatiewet te wijzigen, zodat AT als toezichthoudende autoriteit inzage kan verkrijgen in telecommunicatiegegevens die door de aanbieders worden bewaard of verstrekt, indien en voor zover dat nodig is om het toezicht uit te kunnen oefenen. Met een dergelijke wijziging kan beter toezicht worden uitgeoefend op een rechtmatige en zorgvuldige verwerking van de bewaarde gegevens, inclusief de daadwerkelijke vernietiging daarvan. Met een beter toezicht op de naleving van de wettelijke voorschriften wordt tevens tegemoet gekomen aan het arrest van het Hof van Justitie.

6. De effecten voor de in Nederland opererende telecombedrijven en andere bedrijven

De in paragraaf 5 van deze brief voorgestelde maatregelen zullen gevolgen kunnen hebben voor de bedrijfsvoering van de in Nederland opererende internet- en telecomaanbieders. De verplichting tot opslag van de gegevens op het grondgebied van de Europese Unie kan consequenties hebben voor de bedrijfsvoering en de kosten van de aanbieders. De precieze bedrijfseffecten en kosten zullen in samenwerking met het bedrijfsleven nader in kaart worden gebracht. Bezien vanuit het perspectief van het functioneren van de interne markt ligt het niet in de lijn der verwachting dat de thans voorgestelde maatregelen onevenredige belemmeringen met zich mee zullen brengen. Hierbij moet ook in aanmerking worden genomen dat de eisen die uit het arrest van het Hof van Justitie voortvloeien voor alle lidstaten gelden zodat deze gelijke weerslag zullen hebben op de nationale wetgevingen op het gebied van de bewaarplicht ten behoeve van de opsporing en vervolging van ernstige misdrijven.

In de brief aan de Tweede Kamer van 16 mei 2014, waarbij de Minister van Economische Zaken het rapport "Meting dataretentie 2013" aanbiedt, is aangegeven dat naast zes grote telecomaanbieders, driehonderdzevendertig middelgrote en kleine aanbieders verplichtingen hebben op het gebied van dataretentie en privacyaspecten. Genoemd is dat het aantal bevragingen van opsporingsdiensten bij deze groep van kleinere partijen beperkt is (ca 2%). Deze groep moet gezien hun beperkte bedrijfsomvang relatief gezien meer kosten en inspanningen leveren om aan de eisen op het gebied van dataretentie en privacy te voldoen. Verder is voor juist deze groep van aanbieders de toepassing en naleving van regels inzake de bewaarplicht complex gebleken. Daarom wordt bezien op welke wijze deze groep van aanbieders zoveel mogelijk kan worden ontzien, door ruimte te bieden om op een zo efficiënt mogelijke wijze aan de bewaarplicht te voldoen.
Met de aanbieders zal worden besproken welke eventuele praktische oplossingen denkbaar zijn om aan de naleving van de wettelijke verplichtingen te voldoen, waarbij onevenredige kosten en inspanningen waar mogelijk vermeden worden.

7. De gevolgen van het arrest voor de Nederlandse inlichtingen- en veiligheidsdiensten

De richtlijn dataretentie liet de lidstaten de nodige ruimte voor de regeling van de toegang tot de bewaarde telecommunicatiegegevens. De lidstaten dienden te waarborgen dat de bewaarde gegevens alleen in welbepaalde gevallen en in

overeenstemming met de nationale wetgeving aan de bevoegde nationale autoriteiten werden verstrekt.

Op grond artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) zijn de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) bevoegd zich te wenden tot de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten met het verzoek gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. De desbetreffende aanbieders zijn op grond van artikel 13.4, eerste lid, van de Telecommunicatiewet verplicht om onverwijld aan een dergelijk verzoek te voldoen. Hierin verandert niets. In het kader van de herziening van de Wiv 2002 zal de regering nader in gaan op de mogelijke gevolgen van de uitspraak van het Hof van Justitie voor de werkzaamheden van de inlichtingen- en veiligheidsdiensten.

8. Welke gevolgen heeft de uitspraak voor brede vormen van opslag van persoonsgegevens door de overheid die nu al bestaan en die de regering nog beoogt in te voeren?

Naar aanleiding van de vraagstelling van de vaste commissie voor Veiligheid en Justitie merk ik op dat met de term 'brede vormen van opslag van persoonsgegevens' kennelijk wordt gedoeld op wettelijke regels met betrekking tot de opslag van gegevens voor strafrechtelijke doeleinden omtrent personen, ten aanzien van wie er (op dat moment) geen aanwijzingen zijn van betrokkenheid bij strafbare feiten. Een dergelijke opslag is aan de orde in het voorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie (33 542), ook bekend als het wetsvoorstel ANPR.
Het wetsvoorstel ANPR voorziet in een wettelijke basis voor het bewaren van bepaalde kentekengegevens van alle voertuigen die een camera passeren. Dit betreft het kentekennummer, een foto van het voertuig, het tijdstip en de locatie. De bewaartermijn is vier weken. De gegevens mogen worden geraadpleegd voor de opsporing van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten en voor de aanhouding van een voortvluchtige verdachte of veroordeelde. De gegevens mogen alleen worden geraadpleegd door een daartoe geautoriseerde opsporingsambtenaar, ten behoeve van het opsporingsonderzoek. Koppeling van de bewaarde kentekengegevens met bestanden buiten de politie, om personen in beeld te kunnen krijgen ten behoeve van de opsporing ('dataminen'), is niet mogelijk. De tekst van het voorgestelde artikel 126jj van het Wetboek van Strafvordering sluit dit uit.

Het wetsvoorstel vertoont een belangrijke overeenkomst met de richtlijn dataretentie, omdat kentekens worden vastgelegd van alle passerende voertuigen, inclusief die van personen voor wie er op het moment van vastlegging geen enkele aanwijzing bestaat dat hun gedrag verband vertoont met zware criminaliteit. De Afdeling advisering wijst hier ook op en merkt op dat het aan de wetgever en uiteindelijk aan de rechter is om over dit voorstel een definitief oordeel te geven, maar rekening te houden met de mogelijkheid dat dit soort gegevensopslag zal kunnen worden beoordeeld als strijdig met het evenredigheidsbeginsel of als niet relevant en bovenmatig, uitgaande van het strafrechtelijke doel van de opslag. Er zijn echter aanzienlijke verschillen tussen de richtlijn dataretentie, die aan het oordeel van het Hof van Justitie is

onderworpen, en het wetsvoorstel ANPR. Dit betreft in de eerste plaats de aard van de te bewaren gegevens. Anders dan bij telecommunicatiegegevens, waarmee een meer omvattend beeld kan worden verkregen van de gedragingen van burgers, kunnen kentekengegevens geen zeer nauwkeurige aanwijzingen verschaffen over het privéleven van degenen wier gegevens worden bewaard, zoals de gewoonten van het dagelijkse leven, de plaatsen van permanent of tijdelijk verblijf, de dagelijkse verplaatsingen of verplaatsingen van andere aard, de uitgeoefende activiteiten, de sociale relaties en de gefrequenteerde sociale milieus. De kentekengegevens geven uitsluitend inzicht in de locatie waar een kenteken van een voertuig op een bepaalde datum en tijdstip door een camera is geregistreerd. Op basis van de bewaarde kentekengegevens kan weliswaar inzicht worden verkregen in de locatie van een voertuig op bepaalde data of tijdstippen, maar wordt geen inzicht verkregen in betrekkingen tussen personen. Vanwege hun aard zijn deze gegevens minder ingrijpend voor de persoonlijke levenssfeer. Van essentieel belang is voorts dat de in het wetsvoorstel ANPR voorgestelde bewaartermijn van vier weken voor kentekengegevens aanzienlijk korter is dan de in de richtlijn dataretentie opgenomen bewaartermijn van ten hoogste twee jaar voor de telecommunicatie verkeersgegevens. Hier komt bij dat de kentekengegevens langs de openbare weg worden verzameld. De bestuurders van voertuigen kunnen weten en verwachten dat hun voertuig op de openbare weg aan de hand van het kenteken door de politie kan worden waargenomen, met het oog op de handhaving van wet- en regelgeving. Mede in het licht van het beginsel van de 'reasonable expectation of privacy' van de betrokkene dient het verzamelen en bewaren van kentekengegevens anders te worden gewaardeerd dan het verzamelen en bewaren van telecommunicatiegegevens.

Anders dan bij de bewaarplicht van telecommunicatiegegevens is de toegang tot de bewaarde kentekengegevens echter niet afhankelijk gesteld van voorafgaande toetsing door een rechterlijke instantie of een onafhankelijke administratieve instantie, als bedoeld door het Hof van Justitie (punt 62). Ik ben van oordeel dat, nu de inbreuk op de persoonlijke levenssfeer minder ingrijpend is dan bij de bewaarplicht van telecommunicatiegegevens, het niet strikt noodzakelijk is om ook bij de bewaring van kentekengegevens in een dergelijke waarborg te voorzien. Net als bij de telecommunicatiegegevens geldt dat de kentekengegevens specifiek ten behoeve van de opsporing en vervolging van misdrijven worden bewaard. Met het oog op die overeenkomst ben ik voornemens de toegang tot de bewaarde kentekengegevens afhankelijk te stellen van een voorafgaand bevel van de officier van justitie. Het vereiste van een bevel van de officier van justitie geldt eveneens voor de inzet van andere bijzondere opsporingsbevoegdheden, zoals de stelselmatige observatie, de stelselmatige inwinning van informatie en de infiltratie. Omdat de inzet van deze bevoegdheden een verdergaande inbreuk op de privacy van de betrokken personen vormen dan het bewaren van kentekengegevens van voertuigen - zo kunnen op basis van een bevel tot observatie het gedrag van een persoon gedurende een periode van drie maanden worden waargenomen - ben ik van oordeel dat met een dergelijk vereiste ruimschoots wordt voldaan aan de eisen die voortvloeien uit het Handvest van de grondrechten. Aldus zal in het Wetboek van Strafvordering worden geregeld dat de vordering van de bewaarde kentekengegevens afhankelijk is van een voorafgaand bevel van de officier van justitie. Dit betekent dat het voorgestelde artikel 126jj van het Wetboek van Strafvordering wordt gewijzigd, zodat de daartoe geautoriseerde opsporingsambtenaar slechts op bevel van de officier van justitie de bewaarde kentekengegevens kan raadplegen, met

het oog op de opsporing van een ernstig misdrijf of de aanhouding van een voortvluchtige persoon.

De toegang tot de bewaarde kentekengegevens ten behoeve van de opsporing en vervolging van strafbare feiten is beperkt tot gevallen waarin sprake is van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren. In het licht van de door het Hof van Justitie gestelde eisen aan de toegang tot bewaarde telecommunicatiegegevens, is de regering van oordeel dat deze regeling voldoet aan de te stellen eisen op basis van het EVRM of – voor zover dat van toepassing zou zijn - het Handvest van de grondrechten.
Zoals ik reeds eerder, bij brief van 10 april 2013 (Kamerstukken II, 2013/14, 33 542, nr. 13), heb aangegeven blijft het wetsvoorstel naar mijn stellige overtuiging – zeker met de nadere beperking van de toegang tot de gegevens - dan ook ruimschoots binnen de grenzen van artikel 8 van het EVRM en – voor zover van toepassing - de artikelen 7 en 8 van het Handvest van de grondrechten.

9. Tot besluit

De regering is aldus voornemens de nationale wetgeving inzake de bewaarplicht voor telecommunicatiegegevens aan te passen, zodat:

- de vordering van de officier van justitie tot het verstrekken van telecommunicatiegegevens slechts kan worden gegeven na een voorafgaande machtiging door de rechter-commissaris. Dit betekent dat de regeling van artikel 126n/u van het Wetboek van Strafvordering wordt gewijzigd;

- de toegang tot de gegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven wordt gedifferentieerd aan de hand van de ernst van het misdrijf. Dit betekent dat de regeling van artikel 126n/u van het Wetboek van Strafvordering wordt gewijzigd;

- onderzocht zal worden of de telecommunicatiegegevens, die worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven, kunnen worden versleuteld zodat deze zijn afgeschermd van inzage door onbevoegden. Dit kan leiden tot wijziging van het Besluit beveiliging telecommunicatiegegevens;

- de aanbieders worden verplicht de te bewaren gegevens op het grondgebied van de Europese Unie te bewaren. Dit betekent dat de regeling van de artikelen 13.2a en 13.5 van de Telecommunicatiewet wordt gewijzigd;

- AT als toezichthoudende autoriteit inzage kan verkrijgen in telecommunicatiegegevens die door de aanbieders worden bewaard of verstrekt, met het oog op een beter toezicht op de verwerking van de te bewaren gegevens, en de vernietiging daarvan. Dit betekent dat artikel 18.7, tweede lid, van de Telecommunicatiewet wordt gewijzigd;

Deze aanpassingen zullen worden opgenomen in een voorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering, dat binnenkort in consultatie zal worden gegeven.

Tevens is de regering voornemens het wetsvoorstel inzake de bewaring van kentekengegevens aan te passen, zodat:

- de daartoe geautoriseerde opsporingsambtenaar uitsluitend op bevel van de officier van justitie de bewaarde kentekengegevens kan raadplegen, met het oog op de opsporing van een ernstig misdrijf of de aanhouding van een voortvluchtige persoon. Dit betekent dat het voorgestelde artikel 126jj van het Wetboek van Strafvordering wordt gewijzigd.

Deze aanpassing(en) zullen worden opgenomen in een nota van wijziging bij het wetsvoorstel ANPR, die binnen binnenkort bij Uw Kamer zal worden ingediend.

Ik hoop u hiermee voldoende te hebben ingelicht.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

Directie Wetgeving en Juridische Zaken
Sector straf- en sanctierecht

Datum
17 november 2014

Ons kenmerk
586638