Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 537

Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunicatiegegevens)

Nr. 7

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 maart 2018

1. Inleiding

Met de wet van 18 juli 2009 is in Nederland een algemene bewaarplicht voor telecommunicatiegegevens geïntroduceerd.[1] Deze wet beoogde te garanderen dat bepaalde telecommunicatiegegevens beschikbaar waren voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit (dataretentie). Dit betreft gegevens ter identificatie van gebruikers (hierna: gebruikersgegevens) en verkeers- en locatiegegevens, die aangeven wie, waar, wanneer en met wie in contact is geweest.[2] Dit betreft dus in geen geval de inhoud van de communicatie. Bij verschillende gelegenheden is het belang van een dergelijke bewaarplicht voor de criminaliteitsbestrijding onderstreept.[3] Met de bewaarplicht werd zeker gesteld dat bepaalde telecommunicatiegegevens voor een bepaalde duur beschikbaar waren voor de opsporing en vervolging van ernstige strafbare feiten, waarbij toegang tot de gegevens met strikte waarborgen was omgeven. De algemene bewaarplicht is van belang, omdat in een opsporingsonderzoek juist in een later stadium kan blijken dat bepaalde telecommunicatiegegevens van grote waarde zijn voor de waarheidsvinding, zonder dat op het moment van de vastlegging van de gegevens al sprake is van inzicht in de betrokkenheid van bepaalde personen bij ernstige misdrijven.

[1] *Stb.* 2009, nr. 333.

[2] Gegevens ter identificatie van gebruikers zijn gegevens die nodig zijn om de abonnee of gebruiker van een communicatiedienst te identificeren, zoals naam en adres. Verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie, zoals datum, tijdstip en duur van de communicatie. Locatiegegevens zijn gegevens waarmee de geografische positie van de communicatie apparatuur kan worden bepaald aan de hand van de gebruikte zendmast.

[3] Zie bijvoorbeeld Kamerstuk 33 542, nr. 16 en de bijlage bij Kamerstuk 33 870, nr. 3.

kst-34537-7
ISSN 0921 - 7371
's-Gravenhage 2018

Op 21 december 2016 heeft het Europees Hof van Justitie (hierna: het Hof), volgend op de uitspraak van het Hof uit 2014 in de zaken Digital Rights Ireland en Seitlinger (zaken C-293/12 en 594/12), in de gevoegde zaken Tele2 Sverige AB en Watson (zaken C-203/15 en C-698/15) opnieuw een arrest gewezen over (onder meer) het bewaren van telecommunicatiegegevens. Mede naar aanleiding van dit arrest heeft de vaste commissie voor Veiligheid en Justitie uit de Tweede Kamer, bij brief van 23 december 2016, de toenmalige Minister van Veiligheid en Justitie verzocht de Tweede Kamer een reactie te doen toekomen op het bericht «Europees Hof maakt gehakt van volledige bewaarplicht» (volkskrant.nl, 21 december 2016) en daarbij uiteen te zetten wat de eventuele consequenties zijn voor het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens (Kamerstuk 34 537, nr. 2) dat thans in de Tweede Kamer aanhangig is. Bij brief van 2 februari 2017 heeft de toenmalig Minister van Veiligheid en Justitie een voorlopige reactie op dat verzoek gegeven. Daarbij is bericht dat de gevolgen van het arrest nader moesten worden onderzocht en dat, zodra meer inzicht bestaat in de consequenties van het arrest voor het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens (Kamerstuk 34 537, nr. 2) en de positie van de andere lidstaten van de Europese Unie, het parlement daarover nader zou worden geïnformeerd (Kamerstuk 34 537, nr. 6).

Bij brief van 5 oktober 2017 hebben de voorzitters van de vaste commissies voor Immigratie & Asiel / JBZ-Raad en voor Veiligheid en Justitie uit de Eerste Kamer enkele vragen over het onderwerp dataretentie gesteld. Vanwege de inhoudelijk nauwe samenhang tussen deze vragen en voormelde toezegging zijn de door de vaste commissies gestelde vragen in de onderhavige brief betrokken.

Ten slotte heeft het lid Buitenweg (GroenLinks) bij gelegenheid van het Algemeen Overleg ter voorbereiding op de Informele JBZ Raad van 25 en 26 januari 2018 (Kamerstuk 32 317, nr. 505) enkele vragen over dataretentie gesteld die ook in de onderhavige brief worden geadresseerd.

De uitspraken van het Hof verdienden een zeer zorgvuldige bestudering in het licht van de gevolgen ervan voor het genoemde wetsvoorstel.

In de voorliggende brief zal ik, mede namens de Staatssecretaris van Economische Zaken en Klimaat, na een beknopte weergave van de voorgeschiedenis met betrekking tot een bewaarplicht voor telecommunicatiegegevens, ingaan op het arrest van het Hof van Justitie van 21 december 2016, de gevolgen van het arrest voor het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens, het belang van de beschikbaarheid van zogenoemde gebruikersgegevens voor de opsporing van ernstige strafbare feiten en de stand van de besprekingen over het arrest van het Hof op het niveau van de Europese Unie.

Hierbij is tevens betrokken de wijze waarop het huidige kabinet voornemens is om uitvoering te geven aan hetgeen met betrekking tot het bewaren van telecommunicatiegegevens in het Regeerakkoord «Vertrouwen in de toekomst» is aangekondigd.[4]

Mijn belangrijkste conclusie is dat als gevolg van het arrest van het Hof het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens ingrijpend dient te worden aangepast. Ik zal een nota van wijziging in voorbereiding nemen die er in de eerste plaats toe strekt dat de in het wetsvoorstel opgenomen verplichting tot het bewaren van verkeers- en locatiegegevens wordt beperkt tot een aangepaste regeling met betrekking tot uitsluitend gebruikersgegevens, die zal bestaan uit een verplichting voor aanbieders van openbare telecommunicatiediensten tot het beschikbaar houden van dergelijke gegevens om te kunnen voldoen aan een vordering op grond van het Wetboek van Strafvordering tot het herleiden van een gebruiker van een telecommunicatiedienst of netwerk op een bepaald tijdstip. Ik ben voornemens om een nota van wijziging van deze strekking nog dit voorjaar voor advies voor te leggen aan de Afdeling advisering van de Raad van State.

2. Voorgeschiedenis dataretentie

Ter implementatie van de toenmalige Europese richtlijn dataretentie (richtlijn 2006/24/EU) is in Nederland een algemene bewaarplicht voor telecommunicatiegegevens (gebruikers-, verkeers- en locatiegegevens) ingevoerd (Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van richtlijn 2006/24/EU; *Stb.* 2009, nr. 333).

In 2014 heeft het Hof in de gevoegde zaken Digital Rights Ireland en Seitlinger (zaken C-293/12 en 594/12) de Europese richtlijn dataretentie ongeldig verklaard wegens strijdigheid met het EU recht, meer in het bijzonder het Handvest van de grondrechten van de EU. Het Hof oordeelde dat, gelet op alle overwegingen, de wetgever van de EU met de vaststelling van de richtlijn dataretentie de door het evenredigheidsbeginsel gestelde grenzen had overschreden die in het licht van het Handvest van de grondrechten in acht genomen moeten worden. Vervolgens is de Nederlandse wetgeving rond de bewaarplicht door de rechter buiten werking gesteld in een vonnis van de voorzieningenrechter Den Haag van 11 maart 2015 (ECLI:NL:RBDHA:2015:2498). Naar aanleiding van deze ontwikkelingen is, in september 2016, het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens bij de Tweede Kamer ingediend. Dit wetsvoorstel voorziet in een herziening van de wettelijke regeling rond de bewaarplicht voor telecommunicatiegegevens ten behoeve van de opsporing van ernstige misdrijven.

---

[4] In het Regeerakkoord staat met betrekking tot dataretentie de volgende passage: «Het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens wordt heroverwogen. Hierbij verkent het kabinet in hoeverre het Europese recht ruimte biedt voor een afgewogen bewaarplicht voor bepaalde telecommunicatiegegevens, in het bijzonder voor gegevens die strekken tot identificatie van de gebruiker van een communicatiedienst. Bijzondere aandacht gaat daarbij uit naar waarborgen voor de persoonlijke levenssfeer van burgers, beperkte toegang, aangescherpt toezicht, noodzakelijkheid van bewaartermijnen, adequate bescherming en beveiliging van de gegevens en een rapportage- en evaluatieplicht. Alle nieuwe wetgeving waarin gegevensbewaring wordt geregeld ten behoeve van de opsporing van ernstige strafbare feiten zal worden voorzien van passende waarborgen. Ook zal die wetgeving na vijf jaar worden geëvalueerd, waarbij in ieder geval aandacht zal worden besteed aan de effectiviteit en de impact van die wetgeving.»

Vanwege de ongeldigverklaring van de Europese richtlijn dataretentie door het Hof wordt het beleid ter zake dataretentie op EU-niveau thans beheerst door de richtlijn betreffende privacy en elektronische communicatie (richtlijn 2002/58/EG, de e-privacyrichtlijn). Op grond van de e-privacyrichtlijn zijn de aanbieders van telecommunicatiediensten verplicht om telecommunicatiegegevens te wissen of te anonimiseren vanaf het moment dat de gegevens niet langer voor bedrijfsdoeleinden (facturering etc.) noodzakelijk zijn. De e-privacyrichtlijn biedt de lidstaten echter de mogelijkheid tot vaststelling van een bewaarplicht voor telecommunicatiegegevens, voor zover dat een noodzakelijke, evenredige en proportionele maatregel is ten behoeve van de bescherming van bepaalde publieke belangen, waaronder de opsporing en vervolging van strafbare feiten (artikel 15, eerste lid, van de e-privacyrichtlijn). Daarbij dient het Handvest van de grondrechten te worden gerespecteerd, omdat de nationale wetgeving een grondslag vindt in de e-privacyrichtlijn en het beleidsterrein aldus door het EU recht wordt bestreken. Het Handvest van de grondrechten beschermt het recht van eenieder op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie (artikel 7) en op bescherming van de hem betreffende persoonsgegevens (artikel 8, eerste lid). Vrijwel alle lidstaten van de EU hebben voorzien in nationale wetgeving met betrekking tot dataretentie op basis van de e-privacyrichtlijn.

3. Arrest Hof van Justitie in zaken Tele2 Sverige AB en Watson

Op 21 december 2016 heeft het Hof in de gevoegde zaken Tele2 Sverige AB en Watson (zaken C-203/15 en C-698/15) opnieuw een arrest gewezen over het bewaren van telecommunicatiegegevens ten behoeve van opsporing en vervolging van strafbare feiten. Het Hof oordeelde dat de desbetreffende bepalingen uit de e-privacyrichtlijn, tegen de achtergrond van het Handvest van de grondrechten, zich verzetten tegen een nationale regeling die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van *alle* verkeersgegevens en locatiegegevens van *alle* abonnees en geregistreerde gebruikers betreffende *alle* elektronische communicatiemiddelen (punt 112), omdat de regeling verder gaat dan wat strikt noodzakelijk is (punt 107). In het navolgende worden de overwegingen uit voornoemd arrest aangehaald waarin het Hof de onderbouwing van dit oordeel geeft.

Het Hof stelt eerst vast dat een nationale regeling voor de bewaring van verkeers- en locatiegegevens binnen de reikwijdte van de e-privacyrichtlijn valt. Artikel 5, eerste lid, van deze richtlijn bepaalt met name dat de lidstaten het vertrouwelijke karakter van de communicatie via openbare telecommunicatienetwerken en via openbare telecommunicatiediensten en van de daarmee verband houdende verkeersgegevens moeten garanderen (punt 84). De met artikel 15, eerste lid, van de e-privacyrichtlijn aan de lidstaten geboden mogelijkheid de reikwijdte van de verplichting tot waarborging van de vertrouwelijkheid van de communicatie en van de daarmee verband houdende gegevens te beperken, moet strikt worden uitgelegd omdat de verplichting van artikel 5 van die richtlijn anders grotendeels haar inhoud zou verliezen (punt 89). Het beginsel van proportionaliteit brengt met zich mee dat beperking van de bescherming van persoonsgegevens alleen mogelijk is voor zover dit strikt noodzakelijk is (overweging 96). De in casu voorliggende nationale wetgeving voorziet in een algemene en ongedifferentieerde bewaring van *alle* verkeersgegevens en locatiegegevens van *alle* abonnees en geregistreerde gebruikers betreffende *alle* elektronische communicatiemiddelen, en verplicht de aanbieders deze gegevens stelselmatig en voortdurend te bewaren (punt 97). Uit deze gegevens, in hun geheel beschouwd, kunnen volgens het Hof zeer precieze conclusies worden getrokken over het

privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun verblijfplaats, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren (punt 99).[5] De inbreuk van deze regeling op de door de artikelen 7 en 8 van het Handvest beschermde grondrechten is groot en moet volgens het Hof als bijzonder ernstig worden beschouwd. De omstandigheid dat de gegevens worden bewaard zonder dat de gebruikers van de elektronische communicatiediensten hierover worden ingelicht, kan bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (punt 100). Gelet op de ernst van deze inbreuk kan alleen de bestrijding van ernstige criminaliteit een dergelijke maatregel rechtvaardigen (punt 102). Deze doelstelling kan het algemeen en ongedifferentieerd bewaren van alle verkeers- en locatiegegevens echter niet rechtvaardigen, enerzijds omdat de bewaring van die gegevens dan de hoofdregel is terwijl het met de e-privacyrichtlijn ingevoerde stelsel eist dat deze bewaring de uitzondering vormt (punt 104), anderzijds omdat de nationale regeling in geen enkele differentiatie, beperking of uitzondering voorziet naargelang het nagestreefde doel (punt 105). Een dergelijke regeling beperkt de bewaring met name niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaald geografisch gebied en/of een kring van personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit, of op personen van wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij de bestrijding van criminaliteit (punt 106). De regeling gaat aldus verder dan strikt noodzakelijk is (punt 107). Artikel 15 van de e-privacyrichtlijn staat niet in de weg aan de gerichte bewaring van verkeers- en locatiegegevens ter bestrijding van zware criminaliteit, mits de bewaring wordt beperkt tot het strikt noodzakelijke wat betreft de categorieën van te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring (punt 108).

De nationale regeling dient te worden gebaseerd op objectieve elementen waarmee kan worden gemikt op een groep mensen wier gegevens, althans indirect, een band met handelingen van zware criminaliteit aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid kan worden voorkomen. Een dergelijke afbakening zou volgens het Hof aan de hand van een geografisch criterium kunnen worden verricht, wanneer er bijvoorbeeld in een of meer geografische gebieden een hoog risico bestaat dat dergelijke handelingen worden voorbereid of gepleegd (punt 111).

4. Analyse van het arrest en consequenties voor wetsvoorstel 34 537

Het EU recht staat ook na het arrest toe dat lidstaten bepaalde verplichtingen aan de aanbieders van telecommunicatiediensten opleggen tot het bewaren van telecommunicatiegegevens ten behoeve van de opsporing en vervolging van strafbare feiten. Daarbij dient het EU recht, zoals dat in de jurisprudentie van het Hof is uitgelegd, te worden gerespecteerd.

---

[5] «Aan de hand van de te bewaren gegevens kunnen de bron en de bestemming van een communicatie worden opgespoord en geïdentificeerd en kunnen de datum, het tijdstip, de duur en de aard van de communicatie, de communicatieapparatuur van de gebruikers en de locatie van de mobiele communicatieapparatuur worden bepaald. Aan de hand van deze gegevens kan in het bijzonder worden nagegaan met welke persoon en met welk middel een abonnee of geregistreerde gebruiker heeft gecommuniceerd, hoe lang de communicatie heeft geduurd en vanaf welke plaats zij heeft plaatsgevonden. Bovendien kan aan de hand van deze gegevens worden achterhaald hoe vaak de abonnee of de geregistreerde gebruiker gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd» (punt 98).

Uit het arrest van 21 december 2016 kan worden afgeleid dat het Hof een bewaarplicht voor telecommunicatiegegevens, waarbij sprake is van het algemeen en ongedifferentieerd bewaren van alle verkeers- en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronische communicatiemiddelen, in strijd acht met het EU recht, in het bijzonder het Handvest van de grondrechten. Het Hof komt tot dit oordeel op basis van de interpretatie van het vereiste van de proportionaliteit, aan de hand van het criterium van «de strikte noodzaak». Het Hof laat wel ruimte voor een gedifferentieerde bewaarplicht, die bestaat uit gerichte bewaring van verkeers- en locatiegegevens, maar verbindt daaraan als voorwaarde dat een daartoe strekkende regeling moet worden ingevuld op basis van objectieve criteria. Daarbij geeft het Hof in overweging om te kijken naar beperking tot een bepaalde periode, een bepaald geografisch gebied, of een bepaalde kring van personen.

Met dit arrest lijkt het Hof een stap verder te gaan dan het arrest van 8 april 2014 (Digital Rights Ireland en Seitlinger). In laatstgenoemd arrest oordeelde het Hof dat de voormalige Europese richtlijn dataretentie een zeer ruime en bijzonder zware inmenging in de door de artikelen 7 en 8 van het Handvest van de grondrechten met zich bracht, zonder dat deze inmenging nauwkeurig was omkaderd door bepalingen die konden waarborgen dat zij daadwerkelijk beperkt was tot het strikt noodzakelijke (punt 65). Daarbij werden echter tevens strikte criteria geformuleerd voor de toegang tot en het verdere gebruik van de bewaarde gegevens (punt 62). Dit gaf aanleiding tot de interpretatie dat het feit dat de voormalige richtlijn dataretentie geen enkel verband vereiste tussen de opslag van gegevens en het gedrag van personen weliswaar een zeer vergaande inbreuk op de persoonlijke levenssfeer van de betrokkenen kon vormen, maar dat de ernst van die inbreuk kon worden gecompenseerd door het opnemen van passende garanties en waarborgen voor een zorgvuldige wijze van bewaren en verwerken van gegevens, alsmede de toegang tot die gegevens (Kamerstuk 33 542, nr. 16); aldus zou een algemene bewaarplicht binnen de kaders van het EU recht toelaatbaar zijn.

In deze lijn concludeerde eveneens de Advocaat-Generaal in diens advies in de zaak Tele2 Sverige AB, waarin – mede onder verwijzing naar het arrest van het Hof uit 2014 – een algemene bewaarplicht in beginsel toelaatbaar werd geacht en vooral het belang van voldoende waarborgen voor de toegang tot bewaarde gegevens werd benadrukt (ECLI:EU:C:2016:572). Het Hof overwoog evenwel anders: in het arrest van 21 december 2016 achtte het Hof niet alleen een algemene en ongedifferentieerde bewaarplicht voor alle verkeers- en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronische communicatiemiddelen in strijd met het EU-recht, maar herhaalde het Hof tevens het vereiste van strikte regels rond de toegang en het verdere gebruik van de bewaarde gegevens.
De in het wetvoorstel Aanpassing bewaarplicht telecommunicatiegegevens (Kamerstuk 34 537, nr. 2) voorgestelde bewaarplicht omvat de opslag van de categorieën telecommunicatiegegevens, te weten verkeersgegevens en locatiegegevens, waarvan het Hof het algemeen en ongedifferentieerd bewaren ervan niet verenigbaar acht met het EU recht. De bewaarplicht is niet beperkt tot alleen de verkeersgegevens en locatiegegevens die betrekking hebben op bijvoorbeeld een bepaalde periode en/of een bepaald geografisch gebied en/of een kring van personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit, juist omdat een dergelijke beperking ernstig afbreuk doet aan de effectiviteit van een dergelijke maatregel.

Een vraag die door het arrest niet volledig wordt beantwoord, is wat het Hof precies verstaat onder het bewaren van álle verkeers- en locatiegegevens. Mogelijk dat binnen die categorieën gegevens een beperking in de te bewaren gegevens zou kunnen worden gemaakt. Dit vormt een van de punten waarover in het overleg op EU niveau wordt gesproken (zie paragraaf 8).

In het licht van het arrest van 21 december 2016 moet er op dit moment echter ernstig rekening mee worden gehouden dat de in dit wetsvoorstel voorgestelde regeling voor een algemene bewaarplicht niet verenigbaar is met het arrest van het Hof, en aldus met het EU recht.

Op grond van het vorenstaande ben ik van oordeel dat dit wetsvoorstel aanpassing behoeft, in die zin dat dit in sterk afgeslankte vorm wordt voortgezet, bestaande uit de hieronder nader toegelichte voorziening met betrekking tot uitsluitend gebruikersgegevens.

Ik teken daarbij wel aan dat in het rapport van het openbaar ministerie en de politie (bijlage bij Kamerstuk 33 870, nr. 3) het belang van de bewaring van verkeers- en locatiegegevens voor de opsporing van ernstige delicten aan de hand van uitgebreid beschreven casuïstiek ten overvloede wordt onderbouwd. De desbetreffende casuïstiek maakt inzichtelijk op welke wijze deze gegevens een cruciale rol spelen bij het oplossen van zaken. Als in de toekomst, bijvoorbeeld in het kader van de besprekingen op EU-niveau, zou blijken dat een algemene bewaarplicht voor verkeers- en locatiegegevens in enigerlei vorm verenigbaar is met het Europese recht, dan zal ik herinvoering van een dergelijke bewaarplicht opnieuw bespreekbaar maken.

In dit verband is, naast de besprekingen die op EU-niveau plaatsvinden over de precieze betekenis van het arrest van het Hof, relevant het advies van het Hof van 26 juli 2017 ten aanzien van de voorgenomen overeenkomst tussen de Europese Unie en Canada betreffende de doorgifte van persoonsgegevens van passagiers door luchtvaartmaatschappijen (zaak C 1/15). In het advies oordeelde het Hof over een overeenkomst van de EU met Canada over de verstrekking van passagiersgegevens («PNR-gegevens», Passenger Name Records of Passagiersnamen Register) door Europese luchtvaartmaatschappijen aan Canada, met het oog op de bestrijding van terroristische misdrijven en zware grensoverschrijdende criminaliteit. De voorgenomen overeenkomst voorzag in een bewaartermijn van vijf jaar, onder afscherming van de persoonsgegevens na dertig dagen respectievelijk twee jaar. Het Hof stelde vast dat de voorgenomen overeenkomst niet verder gaat dan strikt noodzakelijk is, voor zover zij de doorgifte van de PNR-gegevens van alle luchtreizigers aan Canada toestaat (punt 189). Daarbij liet het Hof de mogelijkheid open van het gebruik van de bewaarde gegevens gedurende het verblijf van een passagier in Canada ten behoeve van de bestrijding van terroristische misdrijven en zware grensoverschrijdende criminaliteit. Voorwaarde was dat op basis van objectieve gegevens kon worden aangenomen dat de PNR-gegevens van één of meer reizigers daadwerkelijk konden bijdragen aan het bereiken van deze doelstelling (punt 201). Van essentieel belang was dat het gebruik van de gegevens tijdens het verblijf van een reiziger in Canada in beginsel werd onderworpen aan een voorafgaande controle door hetzij een rechterlijke instantie, hetzij een onafhankelijke bestuurlijke entiteit, naar aanleiding van een gemotiveerd verzoek (punt 202). Het oordeel van het Hof in deze kwestie laat ruimte voor het bewaren van passagiersgegevens van alle passagiers voorafgaand en gedurende hun verblijf in Canada, op voorwaarde dat de toegang tot de gegevens gedurende het verblijf van een passagier in Canada is onderworpen aan een voorafgaande controle. Dit oordeel van het Hof kan zijn ingegeven

door de aard van de te bewaren persoonsgegevens, die verschilt van verkeers- en locatiegegevens.[6] Ook is mogelijk dat de – naar het lijkt strengere – benadering van het Hof in het arrest van 21 december 2016 mede is ingegeven door de strikte regels die met betrekking tot de opslag van telecommunicatiegegevens uit de e-privacyrichtlijn voortvloeien; het Hof lijkt daaraan althans veel gewicht te hebben gehecht.

Ik verwacht dat de jurisprudentie inzake de verhouding tussen het bewaren van persoonsgegevens van burgers ten behoeve van de opsporing en vervolging van ernstige strafbare feiten en de bescherming van grondrechten, zoals die zijn neergelegd in het Handvest van de grondrechten, zich de komende jaren nog verder zal uitkristalliseren. Dit is ook onderwerp van het overleg op EU niveau. Ik zal uw Kamer langs de gebruikelijke en daartoe geëigende weg over de ontwikkelingen in de besprekingen op EU niveau informeren, door middel van de geannoteerde agenda ter voorbereiding op de JBZ-Raad.

5. De beschikbaarheid van gegevens ter identificatie van de gebruiker van een communicatiedienst (gebruikersgegevens)

In overleg dat na het arrest van het Hof van 21 december 2016 heeft plaatsgevonden, is vanuit de opsporing- en vervolgingspraktijk met klem gewezen op het feit dat dringend behoefte bestaat aan het kunnen herleiden van het gebruik van een communicatiedienst tot een bepaalde gebruiker op een bepaald tijdstip, voorafgaand aan het moment waarop deze behoefte manifest is. Daartoe is het noodzakelijk te kunnen beschikken over gebruikersgegevens. Deze gegevens hebben geen betrekking op de communicatie tussen personen maar slechts op de identificatie van een gebruiker van een elektronische communicatiedienst en het gebruikte apparaat («device»). Het zijn uitsluitend de gegevens die nodig zijn om achteraf te kunnen vaststellen welke persoon op een bepaald tijdstip gebruik heeft gemaakt van bijvoorbeeld een specifiek IP-adres of telefoonnummer. De bewaarplicht als vervat in het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens omvat thans de verplichting tot het bewaren van gebruikersgegevens. In zoverre is dat niet nieuw. Ik ben voornemens om dit onderdeel van het wetsvoorstel te behouden.

De op dit punt in het wetsvoorstel voorgestelde regeling behoeft evenwel aanpassing in het licht van technologische ontwikkelingen rond het gebruik door aanbieders van telecommunicatiediensten van IP-adressen. Het kunnen beschikken over gebruikersgegevens is van cruciaal belang voor de opsporing en vervolging van ernstige strafbare feiten, in het bijzonder strafbare feiten waarbij gebruik wordt gemaakt van het internet, en waarbij het IP-adres in de regel het enige spoor voor de opsporing vormt. Dit is in een groeiend aantal zaken aan de orde, denk bijvoorbeeld aan de meeste cyberdelicten, waaronder ransomware, ddos-aanvallen en banking malware, maar in het bijzonder ook bij kinderpornografie en grooming. Voorts kennen ook klassieke delicten steeds vaker een digitale component, zoals fraude op internet en grootschalige online handel in wapens en illegale goederen via darkweb, maar ook ernstige bedreigingen en online misbruik van seksueel beeldmateriaal, zoals bij

[6] Het Hof overwoog dat bepaalde PNR-gegevens op zichzelf beschouwd weliswaar geen belangrijke informatie lijken te kunnen verschaffen over het privéleven van de betrokkene maar samen beschouwd onder meer een volledige reisroute kunnen blootleggen, inzicht geven in reisgewoonten en relatie tussen twee of meer personen, inlichtingen verschaffen over de financiële situatie van luchtreizigers, hun voedingsgewoonten of hun gezondheidstoestand en zeer gevoelige gegevens over deze passagiers bevatten (punt 128). Wel is de aard van deze informatie beperkt tot bepaalde aspecten van het privéleven, die in het bijzonder verband houden met luchtreizen tussen Canada en de Unie (punt 150).

zogenoemde wraakporno. Met de voortschrijdende digitalisering neemt de urgentie hiervan alleen maar toe. Op dit moment blijven ernstige strafbare feiten, zoals kinderpornografie en ander seksueel kindermisbruik via het internet, onopgehelderd en onbestraft omdat een essentieel aanknopingspunt voor de opsporing, een IP-adres of telefoonnummer, niet tot een gebruiker te herleiden is. De samenleving verwacht van de overheid dat deze optreedt tegen ernstige normschendingen en slachtoffers beschermt, maar het gebruik van digitale middelen maakt dit op dit moment echter vrijwel onmogelijk. Vanuit het oogpunt van de bescherming van burgers tegen ernstige criminaliteit acht ik dit niet aanvaardbaar. Effectieve mogelijkheden tot het identificeren van de gebruiker van een communicatiedienst zijn nodig om te voorkomen dat het internet een vrijplaats wordt voor de plegers van deze feiten. Daarbij dienen de grondrechten van burgers, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, in acht te worden genomen en zijn passende waarborgen nodig ter bescherming tegen een disproportionele of anderszins onrechtmatige aantasting van deze rechten.

De opsporingsinstanties en het openbaar ministerie zien zich in dit verband, meer in het bijzonder bij het herleiden van een gebruiker van mobiel internet, geconfronteerd met het gevolg van de toepassing door aanbieders van de zogenoemde NAT-technologie (Network Address Translation). Bij deze in Nederland breed toegepaste technologie wordt, om bedrijfsmatige redenen, door aanbieders één publiek IP-adres opgedeeld tussen meerdere (in potentie duizenden) gebruikers.

In de praktijk leidt dit ertoe dat aanbieders thans bij een verzoek van een officier van justitie of een opsporingsambtenaar tot het herleiden van een gebruiker van een mobiel IP-adres niet aan het verzoek kunnen voldoen of dat in een voorkomend geval vele tientallen tot honderden gebruikers door de aanbieder worden aangeleverd. Dit maakt het vorderen van de gegevens inefficiënt en dikwijls zinloos. Door technologische ontwikkelingen is het mogelijk deze identificatie belemmerende omstandigheden te verkleinen, waardoor ik vanuit het eerdergenoemde perspectief van de bescherming van de samenleving voortzetting van de huidige situatie niet langer aanvaardbaar acht. Maatregelen zijn nodig om hierin verbetering te brengen, vergezeld van passende waarborgen ter bescherming van de rechten van burgers.

Ter illustratie van het opsporingsbelang dat met de beschikbaarheid van gebruikersgegevens gemoeid is, geef ik graag twee voorbeelden. In het advies over het conceptwetsvoorstel van het College van Procureurs-Generaal, is destijds melding gemaakt van een internationaal onderzoek naar kindermisbruik, waarin het buitenlandse opsporingsinstanties was het gelukt om zeer veel IP-adressen van gebruikers te achterhalen. In het bestand bevonden zich IP-adressen, die erop wezen dat meer dan honderd Nederlanders mogelijk betrokken waren. Geen van deze zaken kon in behandeling worden genomen omdat de bewaartermijn was verlopen en dus de enige aanknopingspunten om vast te kunnen stellen of, en in welke mate, er betrokkenheid van Nederlanders was, te weten de IP-adressen, niet meer beschikbaar waren.

Voorts wijs ik op een onderzoek naar de illegale handelsplaats Hansa Market. In juli 2017 heeft de politie in samenwerking met de Duitse, Litouwse en Amerikaanse opsporingsdiensten deze illegale handelsplaats op het internet een maand lang overgenomen en in de lucht gehouden. Op de website werd naast drugs ook gehandeld in gestolen juwelen, hackingtools, digitale gegevens en nagemaakte goederen zoals vals geld en valse documenten. Op andere, soortgelijke, websites bieden verkopers eveneens illegale diensten als hacking aan of verboden goederen als

wapens, grondstoffen voor drugs, creditcardgegevens of kinderporno. Om dergelijke websites op te sporen probeert de politie de IP-adressen die gelieerd zijn aan deze websites te achterhalen en hier nader onderzoek naar te doen. Als de provider aan wie een dergelijk IP-adres toebehoort niet kan aangeven aan welke individuele gebruiker dat adres op dat moment was toegekend loopt dat spoor, dat vrijwel altijd het enige spoor is, voor de politie dood en kan de handelsplaats niet worden opgerold met als gevolg dat kopers en verkopers vrij spel hebben.

Concluderend, ik ben overtuigd van de onmisbaarheid en het belang van een verplichting voor aanbieders van telecommunicatiediensten om te voldoen aan het verzoek tot het herleiden van een gebruiker van een telecommunicatiedienst op een bepaald tijdstip. Deze verplichting impliceert dat de betreffende gebruikersgegevens voor een bepaalde termijn beschikbaar worden gehouden voor de opsporing. Dit vereist een wettelijke voorziening. Daarbij zal ik ook de consequenties voor aanbieders van openbare telecommunicatiediensten die NAT-technologie aanbieden, in beschouwing nemen.

6. Een wettelijke regeling voor gebruikersgegevens in het licht van het arrest van het Hof

Een wettelijke voorziening voor beschikbaar houden van gebruikersgegevens is naar mijn overtuiging verenigbaar met het EU-recht en het Handvest van de grondrechten. In het arrest van 21 december 2016 legt het Hof de nadruk op de privacy gevoeligheid van de *verkeers- en locatiegegevens*.

Gebruikersgegevens worden in het arrest niet genoemd. Volgens het Hof kunnen, zoals hierboven weergegeven, uit een combinatie van verkeers- en locatiegegevens, in hun geheel beschouwd, zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. Volgens het Hof kan dit leiden tot een gevoel van permanente surveillance en bestaat het risico van een «chilling effect» op het gebruik door personen van telecommunicatiediensten. De kritiek van het Hof op een algemene bewaarplicht voor alle verkeers- en locatiegegevens is, zo kan uit het arrest worden afgeleid, overwegend door deze zorg ingegeven.

Voor de specifieke categorie van gebruikersgegevens ligt dit wezenlijk anders. Deze gegevens hebben geen betrekking op het inhoudelijk gebruik van een communicatiedienst, noch op de personen met wie de gebruiker contact heeft, hoe lang diens gesprekken zijn of de locatie van de gebruiker. 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 aan de orde was bij de bewaring van de verkeers- en locatiegegevens.

Het beschikbaar houden van gebruikersgegevens van telefonie en internet heeft uitsluitend tot doel om achteraf te kunnen vaststellen welke persoon op een bepaald tijdstip gebruik heeft gemaakt van het telefoonnummer of IP-adres dat is aangetroffen in een strafrechtelijk onderzoek. De inbreuk op de privacy door een verplichting voor aanbieders van telecommunicatie om IP-adressen en telefoonnummers te kunnen herleiden tot een gebruiker, heeft geen betrekking op de communicatie tussen personen en is dus van een geheel andere orde dan bij het bewaren van verkeers- en locatiegegevens.

Er kan, kortom, ook in het licht van het arrest van het Hof een duidelijk onderscheid worden gemaakt tussen enerzijds verkeers- en locatiegegevens en anderzijds gebruikersgegevens. De kaders van het EU recht bieden ruimte voor een wettelijke regeling met betrekking tot deze specifieke categorie telecommunicatiegegevens.

Ook in de besprekingen op EU niveau tekent zich consensus af met betrekking tot het standpunt dat gebruikersgegevens als een specifieke categorie telecommunicatiegegevens moeten worden beschouwd, waarvoor geldt dat geen sprake is van een inbreuk op de privacy van de aard en omvang als die welke onderwerp vormde van het arrest van het Hof van 21 december 2016. De categorie gebruikersgegevens, met andere woorden, valt buiten de reikwijdte van het arrest. Een afgewogen bewaarplicht voor gebruikersgegevens is noodzakelijk en effectief, terwijl de inbreuk op de privacy van burgers bij het bewaren van deze gegevens gering is.

7. Conclusie: nota van wijziging bij wetsvoorstel 34 537

In het licht van het bovenstaande en ter uitvoering van het Regeerakkoord ben ik voornemens om het wetvoorstel Aanpassing bewaarplicht telecommunicatiegegevens (Kamerstuk 34 537) ingrijpend aan te passen.

Ik zal een nota van wijziging in voorbereiding nemen die er in de eerste plaats toe strekt dat de in het wetsvoorstel opgenomen verplichting tot het bewaren van verkeers- en locatiegegevens wordt beperkt tot een aangepaste regeling voor het bewaren gebruikersgegevens, die – in de kern – zal bestaan uit een verplichting voor aanbieders van openbare telecommunicatiediensten om dergelijke gegevens beschikbaar te houden teneinde te kunnen voldoen aan een vordering op grond van het Wetboek van Strafvordering tot het herleiden van een gebruiker van een telecommunicatiedienst op een bepaald tijdstip.

In het licht van vorenstaande is het wetsvoorstel in een dergelijke, sterk ingeperkte vorm naar mijn overtuiging zonder meer verenigbaar met het EU recht. Ik ben voornemens om de nota van wijziging op korte termijn voor advies aan de Afdeling advisering van de Raad van State voor te leggen, conform de toezegging in het nader rapport bij het wetsvoorstel (Kamerstuk 34 537, nr. 4, p. 4).

Separaat aan voortzetting van het wetsvoorstel, dat zich straks dus beperkt tot alleen een regeling ter zake gebruikersgegevens, wil ik de besprekingen op EU-niveau voortzetten voor een eenduidig en Europees antwoord op de vraag welke mogelijkheden, met inachtneming van de door het Hof gestelde voorwaarden, resteren tot het bewaren van verkeers- en locatiegegevens. Mocht dit in de toekomst leiden tot een bestendige lijn, dan ligt het naar mijn mening in de rede dat de Europese Commissie een voorstel voor een Europees instrument met betrekking tot dataretentie doet.

8. Stand van zaken besprekingen op EU niveau

Op EU niveau wordt, zoals ik uw Kamers ook via de reguliere informatievoorziening rondom de JBZ Raden heb bericht, binnen het verband van de JBZ-Raad tussen de lidstaten gesproken over het arrest van het Hof, de gevolgen daarvan voor de nationale wetgeving in de verschillende lidstaten en de resterende mogelijkheden, binnen de kaders van het EU recht, tot dataretentie. Ook Eurojust, Europol en de Commissie participeren in het overleg.

Nederland heeft dit initiatief verwelkomd, omdat overleg met de andere lidstaten essentieel is voor het verkrijgen van inzicht in de consequenties van het arrest en een gecoördineerde EU aanpak rond de dataretentie. De besprekingen zijn verkennend van aard en strekken tot gemeenschappelijke duiding van (de gevolgen van) het arrest van het Hof.

De besprekingen op EU niveau hebben duidelijk gemaakt dat alle lidstaten de beschikbaarheid van telecommunicatiegegevens van groot belang beschouwen voor de opsporing en vervolging van ernstige strafbare feiten en terrorismebestrijding. Er leven dan ook breed zorgen over de gevolgen van het arrest voor de mogelijkheden tot gebruik van telecommunicatiegegevens ten behoeve van de opsporing en vervolging van ernstige strafbare feiten en terrorismebestrijding. De Europese Raad heeft in zijn conclusies van 22 en 23 juni 2017 hiervoor aandacht gevraagd. Deze zorgen worden ook gedeeld ten aanzien van de taakuitvoering van de Europese inlichtingen- en veiligheidsgemeenschap, waaronder ook de AIVD en MIVD.

Als voorlopige uitkomst geldt dat de lidstaten in zijn algemeenheid sceptisch staan tegenover de suggestie van het Hof om te voorzien in een specifieke bewaarplicht voor verkeers- en locatiegegevens die zich beperkt tot een bepaald geografisch gebied of een bepaalde kring van personen. De essentie van een dergelijke bewaarplicht is juist dat die algemeen is; het laat zich immers niet op voorhand voorspellen welke personen als dader of slachtoffer betrokken zullen raken bij ernstige criminaliteit. Daar komt bij dat de door het Hof in overweging gegeven benadering, bestaande uit differentiatie naar een bepaald geografisch gebied of een bepaalde kring van personen, in potentie tot stigmatisering of zelfs een discriminatoir effect zal kunnen leiden, bijvoorbeeld als een bepaalde wijk of een bepaalde categorie gebruikers zou worden aangewezen die onder een bewaarplicht worden gebracht.

De praktische bezwaren van zo'n benadering nog daargelaten. Lidstaten vrezen voorts voor verplaatsingseffecten bij een gedifferentieerde bewaarplicht; criminelen zullen hun communicatie – meer nog dan nu – aanpassen en gebruik gaan maken van communicatiediensten die niet onder de gedifferentieerde bewaarplicht vallen. De besprekingen richten zich dan ook op de vraag in hoeverre langs andere weg, binnen de kaders van het EU recht, tot een bewaarplicht kan worden gekomen.

Voorts lijkt er, zoals hierboven reeds werd aangestipt, op EU niveau consensus over te bestaan dat *gebruikersgegevens* buiten de reikwijdte van het arrest van het Hof vallen, omdat het bewaren van dergelijke gegevens een geringe inmenging in de persoonlijke levenssfeer van de gebruiker vormt. In het voortgangsverslag dat onder het toenmalige Maltese voorzitterschap tijdens de JBZ Raad van juni 2017 is vastgesteld, is deze gedeelde zienswijze neergelegd.

Tijdens de JBZ Raad van december 2017 is besloten dat de besprekingen op EU niveau onder Bulgaars voorzitterschap zullen worden voortgezet. Er is een aantal elementen benoemd die nader besproken moeten worden, waaronder de relatie tussen dataretentie en de bepalingen uit de toekomstige e-privacyverordening. Graag verwijs ik in dit verband verder naar het verslag van de desbetreffende JBZ Raad.

Overigens richten de besprekingen op EU niveau zich – gegeven de voormelde consensus ten aanzien van de categorie gebruikersgegevens – thans primair op de verkeers- en locatiegegevens. Separaat aan het voorbereiden van de nota van wijziging met betrekking tot het wetsvoorstel met Kamerstuk 34 537 wil ik de besprekingen op EU niveau

vervolgen en de uitkomst daarvan afwachten voor een eenduidig antwoord op de vraag welke mogelijkheden, binnen de kaders van het EU recht, resteren tot het bewaren van verkeers- en locatiegegevens.

Ik zal het parlement langs de gebruikelijke en daartoe geëigende weg over de ontwikkelingen in de besprekingen informeren, door middel van de geannoteerde agenda ter voorbereiding op de JBZ-Raad.

9. Overig

In reactie op een vraag van de vaste commissies voor Immigratie & Asiel / JBZ-Raad en voor Veiligheid en Justitie uit de Eerste Kamer naar de gevolgen van het arrest van 21 december 2016 voor wetgevingsvoorstellen op nationaal niveau wijs ik in de eerste plaats op de hierboven geschetste consequenties van het arrest voor het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens. Voorts geldt dat de overwegingen van het Hof niet onverkort van toepassing kunnen worden verklaard op andere wetgevings(voorstellen). Daarvoor is de context van dataretentie, waarbinnen het arrest van het Hof is gewezen, te specifiek. Hierboven is reeds het specifieke karakter van gegevens met betrekking tot communicatie aan de orde gekomen. Het arrest vereist een beoordeling per geval, waarbij ter illustratie kan worden gewezen op hetgeen over de verhouding tot het arrest van het Hof naar voren is gebracht in het kader van het toenmalige wetsvoorstel Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie (Kamerstuk 33 542, C).

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus