33870-1 Evaluatie van de Wet bewaarplicht telecommunicatiegegevens

De vaste commissie voor Veiligheid en Justitie heeft een aantal vragen en opmerkingen ter beantwoording voorgelegd aan de minister van Veiligheid en Justitie over evaluatie van de Wet bewaarplicht telecommunicatiegegevens (33870, nr. 1).

Vragen en antwoorden zijn hierna afgedrukt.

Vragen 1, 6, 8 en 13 De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van de evaluatie van de wet. Zij zijn altijd kritisch geweest over de bewaarplicht en vinden een gedegen evaluatie daarom van belang. Daarom is het spijtig dat deze eerste evaluatie veel te laat afgerond is. Wat is de oorzaak van deze vertraging? De leden van de SP-fractie hebben met belangstelling kennisgenomen van de evaluatie van de wet. Zij hebben hierover enkele vragen en opmerkingen. Allereerst wensen zij te vernemen waarom deze evaluatie zo lang op zich heeft laten wachten. Waardoor is zo veel vertraging opgelopen? De leden van de D66-fractie lezen in artikel 13.9 Telecommunicatiewet (Tw) dat de evaluatie in 2011 aan de Tweede Kamer had moeten worden toegezonden. Wat is de reden voor de vertraging? Kan de minister uitleggen waarom de evaluatie van de wet anderhalf jaar te laat aan de Tweede Kamer is aangeboden?
Antwoorden 1, 6, 8 en 13 Het onderzoek is later dan gepland van start gegaan omdat de benodigde expertise bij het WODC niet eerder beschikbaar was. Daarnaast bleek de evaluatie van de Wet bewaarplicht telecommunicatiegegevens dermate complex dat het onderzoek meer tijd in beslag heeft genomen dan vooraf was voorzien.

Vragen 2, 3 en 4. In de inleiding van de evaluatie lezen de leden van de PvdA-fractie met instemming de beschouwing van de directeur van het WODC, waarin hij aangeeft dat het huidige gebruik van mobiele communicatiemiddelen voor steeds meer metadata zorgt, waarmee een compleet beeld van iemand te maken is. Een groot deel van deze metadata wordt in het kader van de bewaarplicht opgeslagen. Ziet de minister het toenemende belang en de toenemende ingrijpendheid van het verzamelen van metadata? Deze leden zijn van mening dat de minister nog zorgvuldiger moet omgaan met de verzamelde gegevens. Deelt de minister deze mening? Hoe wordt deze extra zware zorgplicht ingevuld?
Antwoorden 2, 3 en 4 De regering is overtuigd van het belang en de onmisbaarheid van een bewaarplicht voor telecommunicatiegegevens voor de opsporing en vervolging van ernstige misdrijven.

Daarbij vind ik het belangrijk dat zorgvuldig wordt gekeken naar de gevolgen van de bewaarplicht voor de privacy.
In het arrest van het Hof van Justitie is de richtlijn dataretentie, die is geïmplementeerd in de Wet bewaarplicht telecommunicatiegegevens, ongeldig verklaard. De conclusie van de zorgvuldige analyse van de mogelijke gevolgen van het arrest voor de Nederlandse wetgeving is dat de wetgeving inzake de bewaarplicht van telecommunicatiegegevens aanpassing behoeft. Daartoe is inmiddels een conceptwetsvoorstel opgesteld. Dit conceptwetsvoorstel is als bijlage meegezonden bij de reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie.

Vraag 5, 7, 15 en 28
De voordelen van het systeem zijn duidelijk, maar onduidelijk blijft of de bewaarplicht nodig is. Daarom willen de leden van de PvdA-fractie de regering nogmaals vragen de effectiviteit en de noodzaak helder en ondubbelzinnig uit te leggen.

De leden van de SP-fractie constateren dat volgens de minister uit het onderzoek blijkt dat historische verkeersgegevens over telefonie en internet veelvuldig worden opgevraagd en geanalyseerd voor de opsporing. Dat kan zo zijn, maar deelt de minister de mening dat een veel relevantere vraag is wat al die opvragingen en analyses opleveren?

Kan de minister de noodzakelijkheid van de bewaarplicht onderbouwen?

De leden van de SP-fractie benadrukken dat het WODC schrijft dat het niet mogelijk is om de effecten vast te stellen van de invoering van de wet op het gebruik van verkeersgegevens in de opsporingspraktijk. Hoe gaat de minister nu alsnog aantonen dat zonder deze wet een substantieel aantal strafbare feiten niet zou zijn opgelost?

Antwoord 5, 7, 15 en 28
De bewaarplicht heeft als doel om historische verkeersgegevens gedurende een bepaalde periode beschikbaar te houden voor opsporingsonderzoeken naar ernstige misdrijven. Uit het onderzoek van het WODC en de opsporingspraktijk blijkt dat de bewaarde gegevens veelvuldig in opsporingsonderzoeken worden gebruikt en op verschillende manieren van waarde zijn.

De regering is overtuigd van het belang en de onmisbaarheid van een bewaarplicht voor telecommunicatiegegevens voor de opsporing en vervolging van ernstige misdrijven. Voor een nadere onderbouwing verwijs ik graag naar de reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie (paragraaf 5.2.) en het conceptwetsvoorstel tot 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 elektronische communicatiediensten (paragraaf 5). In die documenten wordt, op basis van een aantal voorbeelden uit de opsporingspraktijk, de noodzaak van de bewaarplicht onderbouwd.

Het afschaffen van de bewaarplicht zou zeer verstrekkende gevolgen hebben voor de opsporing. De gegevens die in het kader van de bewaarplicht worden bewaard zijn onmisbaar en van groot belang voor de opsporing en vervolging van ernstige misdrijven.

Zonder deze gegevens wordt de opsporing van delicten die worden gepleegd op internet of via internet, zoals kinderpornografie, grooming, stalking, digitale diefstal, hacken, digitale aanvallen, ronselen of rekruteren van personen voor de jihad, ernstig belemmerd of zelfs onmogelijk gemaakt. In veel gevallen is het internetspoor, namelijk het IP-adres, het enige spoor.

Ook bij de opsporing van delicten die niet met behulp van internet worden gepleegd, zoals roofovervallen, verkrachtingen, ontvoeringen, moord en doodslag, zijn telecommunicatiegegevens essentieel voor het opsporingsonderzoek. In de meeste gevallen zullen historische telefonie- en internetgegevens pas geruime tijd, soms zelfs maanden na het plegen van het delict worden opgevraagd, omdat bij verreweg de meeste ernstige criminaliteit niet meteen een verdachte in beeld is. Een verdachte komt in de meeste gevallen pas geruime tijd na het moment van het plegen van het delict in beeld door getuigenverklaringen, forensisch onderzoek, het opvragen en onderzoeken van beelden die met bewakingscamera's zijn gemaakt, na onderzoek van het netwerk van het slachtoffer, de gangen van het slachtoffer in de dagen vóór het misdrijf, en dergelijke. Inzicht in de historische gegevens zorgt voor het uitsluiten of juist identificeren van mogelijke verdachten.

Vraag 9
De leden van de D66-fractie horen graag van de minister of het niet tijdig toezenden van een evaluatie vaker voorkomt, welke argumenten daar toen voor golden en of dat overeenkomt met deze situatie.

Antwoord 9
Daarover is geen informatie beschikbaar.

Vraag 10
De leden van de D66-fractie lezen in de brief van de minister dat er enkel gebruikgemaakt zal worden van de gegevens bij een ernstig misdrijf. Kan de minister inzicht geven in de selectiecriteria voor een misdrijf waarbij de gegevens worden geraadpleegd?

Antwoord 10
In het wetboek van Strafvordering is geregeld dat de toegang tot verkeersgegevens voor politie en justitie is beperkt tot gevallen waarin sprake is van ernstige misdrijven. Het gaat om misdrijven waarvoor voorlopige hechtenis mogelijk is, bedoeld in artikel 67, eerste lid, Wetboek van Strafvordering, zoals bijvoorbeeld grooming (digitaal kinderlokken), verkrachting van minderjarigen, bedreiging en mensenhandel.

In het conceptwetsvoorstel wordt de toegang tot de gegevens met betrekking tot (internet)telefonie over een vast of mobiel netwerk ten behoeve van de opsporing van strafbare feiten beperkt aan de hand van de ernst van het betreffende misdrijf. De nadere regeling van de toegang komt op het volgende neer. De bewaartermijn is voor de gegevens met betrekking tot telefonie vastgesteld op twaalf maanden. De gegevens worden bewaard door de telecombedrijven en bevinden zich feitelijk dus ook nog niet bij OM of politie. Om toegang tot die gegevens te verkrijgen is een vordering van de officier van justitie nodig. De bewaartermijn van twaalf maanden kan, anders dan tot nu toe, echter alleen volledig benut worden wanneer sprake is van de zwaarste categorie

delicten, met een strafbedreiging van acht jaar of meer. Bij lichtere delicten, waarvoor voorlopige hechtenis mogelijk is maar waar geen strafdreiging van acht jaar of meer op staat, mogen de gegevens slechts gedurende een periode van zes maanden worden gevorderd. In die laatste situatie zijn de gegevens binnen de bewaartermijn dus nog wel in bezit van de telecomaanbieders, maar kan de officier van justitie ze niet meer vorderen. Dit betekent in feite dat de periode van beschikbaarheid van de bewaarde telefoniegegevens voor de opsporing van ernstige misdrijven, waarvoor voorlopige hechtenis kan worden opgelegd en waarop een maximale gevangenisstraf staat van minder dan 8 jaar, wordt teruggebracht van twaalf naar zes maanden.

Vraag 11
De leden van de D66-fractie krijgen tevens graag inzicht in het afwegingskader dat bij deze misdrijven geldt.

Antwoord 11
Wanneer in het kader van een opsporingsonderzoek behoefte bestaat aan het vorderen van telecommunicatiegegevens, dan wordt de afweging over de toelaatbaarheid van die vordering gemaakt door een officier van justitie. Allereerst geldt dat moet zijn voldaan aan de vereisten zoals die zijn neergelegd in onder meer de artikelen 126n/u of 126na/ua van het Wetboek van Strafvordering. Uitgangspunt bij de daarop volgende afweging of een inzet toelaatbaar is, is dat de inzet moet voldoen aan de vereisten van proportionaliteit en subsidiariteit: de inzet moet (kort gezegd) evenredig zijn aan het misdrijf en er mag geen ander, minder ingrijpend, middel voorhanden zijn waarmee het zelfde doel kan worden bereikt.

In het conceptwetsvoorstel wordt voorgesteld de toegang tot de bewaarde verkeers- en locatiegegevens, op grond van artikel 126n/u Sv, afhankelijk te stellen van een voorafgaande rechterlijke toetsing, zodat beter kan worden gewaarborgd dat de gegevens uitsluitend worden geraadpleegd in de gevallen waarin daartoe voldoende aanleiding bestaat. De rechterlijke toetsing zal worden gewaarborgd door middel van het wettelijke vereiste van een voorafgaande machtiging van de rechter-commissaris.

Vraag 12
De D66-fractie vraagt de minister om een tabel op te stellen met in de eerste kolom alle aanbevelingen uit het onderzoeksrapport, in de tweede kolom de inhoudelijke beleidsreactie en in de derde kolom de actieplannen op dit gebied.

Antwoord 12

Aanbevelingen WODC	Beleidsreactie en actie
p. 77 van het WODC rapport: Het Agentschap Telecom (AT) heeft niet de bevoegdheid om de daadwerkelijke output van verkeers- en locatiegegevens van verschillende aanbieders in te zien. Hiermee mist het AT een instrument om dit aspect van het toezicht goed uit te kunnen voeren. Het verdient daarom	Voorgesteld wordt de tekst van artikel 18.7, tweede lid van de Telecommunicatiewet te wijzigen, zodat het AT kan beschikken over de bewaarde verkeersgegevens, indien en voor zover dat nodig is om het toezicht op de bewaarplicht uit te voeren, bijvoorbeeld om te controleren dat gegevens tijdig zijn

aanbeveling om de rol van de toezichthouder op dit vlak te verbeteren.	vernietigd. Deze bevoegdheid draagt aldus bij aan het verhogen van de bescherming van de privacy van gegevens.
p. 118 van het WODC rapport: Een zorgvuldige heroverweging van de regeling betreffende de te bewaren internetgegevens en de daarbij onlosmakelijk verbonden afweging betreffende de bewaartermijn is wenselijk.	Ten aanzien van de bewaartermijn heeft het Hof van Justitie overwogen dat de richtlijn bepaalde dat de bewaartermijn varieert van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is. De resultaten van het WODC onderzoek en de ervaringen uit de opsporingspraktijk laten zien dat inkorten van de bewaartermijn voor de praktijk zeer onwenselijk is. De huidige bewaartermijnen worden door de opsporing en vervolging als adequaat (telefonie) of zelfs te kort (internet) ervaren. Gegeven de privacy en terughoudendheid die daarbij hoort als reactie op de uitspraak van het Hof en de voorlichting van de Raad van State acht de regering harmonisering van de bewaartermijn, het gelijk trekken naar twaalf maanden voor zowel telefonie als internet, op dit moment niet opportuun. Daarom wordt in het conceptwetsvoorstel voorgesteld de bewaartermijnen onveranderd te laten. Dat wil zeggen, een bewaartermijn van zes maanden voor internetgegevens en twaalf maanden voor telefonie. Naar aanleiding van het arrest van het Hof van Justitie en het WODC onderzoek heeft een evaluatie van de lijst van de te bewaren telecommunicatiegegevens plaatsgevonden. Daarbij is onderzocht welke gegevens strikt noodzakelijk zijn voor het voorkomen, opsporen of vervolgen van ernstige criminaliteit. Dit heeft geleid tot aanpassing en, waar nodig, verduidelijking van de lijst van te bewaren telecommunicatiegegevens.

p. 124 van het WODC rapport: Om in de toekomst een beter beeld te krijgen van het exacte aantal bevragingen dat jaarlijks wordt gedaan, is het van belang de managementsystemen van de ULI (thans: I&S) zodoende aan te passen dat hierover betrouwbaardere gegevens kunnen worden gegenereerd. Daarnaast zou meer inzicht geboden kunnen worden in de mate waarin Nederlandse opsporingsdiensten een inbreuk maken op de privacy van verdachten en betrokkenen door de inzet van dit opsporingsmiddel. Verder zou hierin meer inzicht kunnen worden geboden door de vorderingen zodanig te registreren dat zichtbaar wordt over hoeveel personen er jaarlijks telecommunicatieverkeersgegevens worden opgevraagd, in hoeveel zaken dit gebeurt en voor welke soort zaken deze gegevens worden opgevraagd.	Op grond van de in de Telecommunicatiewet geregelde bewaarplicht moeten gebruikers- en verkeersgegevens worden bewaard door de aanbieders. Het aantal bevragingen van gebruikers- en verkeersgegevens wordt geregistreerd. Op hoeveel politieonderzoeken of aantal personen deze bevragingen betrekking hebben wordt niet geregistreerd. Het publiceren van deze gegevens acht ik onwenselijk omdat met deze verstrekking de belangen van opsporing en vervolging naar mijn mening in de weg kunnen staan en op deze wijze de werkwijzen van politie en justitie openbaar kunnen worden.

Vraag 14

Deelt de minister de mening dat de bewaarplicht door de inperking van de privacy niet alleen nuttig moet zijn maar ook noodzakelijk, om te kunnen voldoen aan de vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens?

Antwoord 14

Ja, die mening deel ik.

Vraag 16

Het valt de leden van de ChristenUnie-fractie op dat er wel wordt gesproken over de bijdrage van de bewaarplicht aan een efficiënte opsporing maar dat in het rapport niet de vraag wordt gesteld of zonder de wettelijke bewaarplicht (of met een minder vergaande bewaarplicht) een serieuze hoeveelheid strafrechtelijke onderzoeken eveneens opgelost zou zijn. Waarom is dit niet onderzocht?

Antwoord 16

Het doel van het WODC onderzoek is inzicht te bieden in de wijze waarop de Wet bewaarplicht telecommunicatiegegevens in de praktijk wordt vormgegeven en in de wijze waarop de gegevens die op grond van die wet worden opgeslagen in de praktijk door politie en justitie worden opgevraagd en gebruikt. Zoals in het rapport ook staat aangegeven is het niet mogelijk om vast te stellen wat de concrete effecten zijn van de

invoering van de Wet bewaarplicht telecommunicatiegegevens op het gebruik van verkeersgegevens in de opsporingspraktijk.
De gegevens worden namelijk veelal gebruikt in combinatie met andere tactische en technische opsporingsinformatie.

De telecommunicatiegegevens waar het hier om draait waren ook voordat de wet werd ingevoerd beschikbaar voor de opsporing en werden ook voor de invoering van de wet gebruikt in strafrechtelijke onderzoeken naar ernstige misdrijven.
Overigens is de situatie van nu anders dan de situatie van vóór de invoering van de bewaarplicht. In 2009 was het voor aanbieders noodzakelijk om voor bedrijfsdoeleinden verkeersgegevens en gebruikersgegevens te bewaren; dat is nu bij veel contracten als gevolg van technologische ontwikkelingen niet meer noodzakelijk. Teruggaan naar de situatie van vóór 2009 is niet mogelijk omdat de omstandigheden wezenlijk zijn veranderd. In de praktijk zou dit bijvoorbeeld tot gevolg kunnen hebben dat de verkeersgegevens en gebruikersgegevens direct nadat de communicatie heeft plaatsgevonden vernietigd worden.

Uit het onderzoek blijkt dat de bewaarde gegevens veelvuldig in opsporingsonderzoeken worden gebruikt en op verschillende manieren van waarde zijn. Daarbij is van belang dat telecomgegevens niet als bewijs hoeven te worden gebruikt om noodzakelijk te zijn. Deze gegevens zijn vaak in het stadium van het ontstaan van de verdenking of voor het kunnen uitsluiten van bepaalde betrokkenen van belang. Daarnaast leiden deze gegevens tot betere beslissingen over het al dan niet inzetten van zwaardere opsporingsmiddelen als de telefoontap en observatie. Slechts in enkele gevallen worden telecomgegevens ook als expliciet bewijsmiddel gehanteerd. Zonder die gegevens zou het stadium van een bewijsbare zaak in veel gevallen wellicht helemaal niet bereikt kunnen worden.

Vragen 17, 19, 56, 57, 58, 59 en 60

De onderzoekers van het WODC constateren de nodige gebreken, zoals een slecht werkend inzagerecht voor burgers en een onvolledig toezicht door het AT. Welke stappen onderneemt de minister om ervoor te zorgen dat deze gebreken worden opgelost en op welk moment verwacht hij alle gebreken te hebben verholpen?

Op welke wijze wordt het instrumentarium van het AT aangevuld?

De leden van de PvdA-fractie lezen in de evaluatie dat het AT onvoldoende bevoegdheden heeft om zijn toezichthoudende rol goed uit te kunnen voeren. Deze leden vinden dit toezicht van groot belang. Schieten de bevoegdheden van het AT inderdaad tekort?

Zo ja, welke maatregelen gaat de minister nemen om hierin te voorzien?

De leden van de SP-fractie ontvangen graag een reactie van de minister op het door de onderzoekers geconstateerde gebrekkige toezicht. Het AT beschikt niet over de bevoegdheden die nodig zijn om op de inhoud van de bewaarde gegevens toe te kunnen zien. Het WODC concludeert dat een overheid die besluit privacygevoelige informatie

van burgers op te slaan en te bewaren, daarop ook solide en effectief toezicht moet organiseren, zowel op de inhoud van de gegevens die worden bewaard als op de gegevens die uiteindelijk aan de opsporingsdiensten worden verstrekt. Wat is de reactie van de minister hierop?

Hoe zal de rol van de toezichthouder eruit komen te zien?

Welke verbeteringen zullen zorgen voor het solide en effectieve toezicht zoals door het WODC aanbevolen?

Antwoorden 17, 19, 56, 57, 58, 59 en 60

In het huidige artikel 18.7, tweede lid, van de Telecommunicatiewet (Tw) wordt uitdrukkelijk bepaald dat de toezichthouders niet bevoegd zijn verkeers- of locatiegegevens op te vragen die door de aanbieders op grond van artikel 13.2a Tw moet worden bewaard. Het toezicht dat AT uitoefent op de beveiliging en vernietiging van gegevens die nodig zijn voor de opsporing bestaat op dit moment daarom uit systeemtoezicht. Dat wil zeggen dat de toezichthouders van AT aan de hand van een beschrijving die de aanbieder geeft van zijn bedrijfsvoeringsprocessen, beoordelen of die aanbieder voldoende maatregelen heeft genomen om de beveiliging en vernietiging van deze gegevens te waarborgen. Deze aanpak betekent dat de toezichthouders niet feitelijk kunnen vaststellen welke gegevens de aanbieder bewaart, hoe deze worden bewaard, hoe ze worden beveiligd en wanneer en hoe ze worden vernietigd. Volgens het WODC mist AT daarmee een instrument om dit aspect van het toezicht goed uit te kunnen voeren.

Gelet op het voorgaande wordt voorgesteld om artikel 18.7, tweede lid Tw te wijzigen om de toezichthouders van AT in staat te stellen om gegevens feitelijk in te zien. Met de voorgestelde wijziging wordt de bescherming van de privacy van degenen op wie deze gegevens betrekking hebben, vergroot. Immers, diegenen zijn er bij gebaat dat de toezichthouders van AT feitelijk kunnen onderzoeken of de verwerking, beveiliging en vernietiging van gegevens plaats heeft conform de wettelijke voorschriften.

Vragen 18, 69, 70, 74, 75 en 77

Op welke termijn kunnen burgers inzage krijgen in alle gegevens die over hen worden verwerkt, zonder daarbij een rechtszaak te moeten beginnen?

Op welke wijze wordt verbetering afgedwongen bij de telecomproviders?

Wanneer krijgen mensen al hun gegevens te zien zodra ze daar naar vragen?

Kunnen klanten alsnog recht op inzage hebben?

De leden van de SP-fractie vragen hoe het kan dat het in de Wet bescherming persoonsgegevens neergelegde recht op inzage in de eigen gegevens in de praktijk niet correct wordt nageleefd.

Hoe garandeert de minister correcte naleving in de toekomst?

Antwoorden 18, 69, 70, 74, 75 en 77

Het CBP heeft aangegeven op korte termijn op zijn website een specifieke modelbrief te publiceren waarmee betrokkenen zich tot hun aanbieder kunnen wenden om hun inzagerecht uit te oefenen. Betrokkenen kunnen het CBP ook een signaal sturen indien hun inzagerecht niet wordt gerespecteerd. Het CBP gebruikt de informatie uit deze signalen voor het maken van keuzes in het kader van zijn toezichthoudende taak. Het CBP doet dit op basis van een risicoanalyse. De ernst van de overtreding en het aantal mensen dat hierdoor wordt geraakt, zijn hierbij belangrijke criteria.

Vraag 20 en 21

De leden van de PvdA-fractie vinden de notificatieplicht van groot belang bij de inzet van bijzondere middelen, omdat deze notificatie de rechtszekerheid van burgers vergroot en de overheid verantwoording aflegt richting burgers. Daarom is de notificatieplicht ook van belang bij het opvragen van informatie die is opgeslagen in het kader van de bewaarplicht. Onderschrijft de minister het belang hiervan?

Zo nee, waarom levert de notificatieplicht volgens de minister geen wezenlijke bijdrage aan de bescherming van de persoonlijke levenssfeer van mensen?

Antwoord 20 en 21

De notificatieplicht is geregeld in het Wetboek van strafvordering. Een wetsvoorstel tot wijziging van de notificatieplicht ligt ter behandeling in de Tweede Kamer. Beantwoording van deze vraag zal bij de Kamerbehandeling van dat wetsvoorstel plaatsvinden.

Vragen 22 en 23

Uit de evaluatie blijkt in ieder geval dat er geen behoefte is aan verdere verlenging van de termijn van een jaar. De leden van de PvdA-fractie vragen of harmonisatie gewenst is. Zij zien de noodzaak van deze harmonisatie niet en vragen de minister welk probleem er met deze harmonisatie opgelost wordt.

Verder constateren zij dat ook een bewaartermijn van zes maanden het merendeel van het gebruik van de opgeslagen gegevens ondersteunt. Is een harmonisatie naar een half jaar daarom geen logische keus?

Antwoorden 22 en 23

Het Hof van Justitie heeft overwogen dat de richtlijn bepaalde dat de bewaartermijn varieert van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is.
De resultaten van het WODC onderzoek en de ervaringen uit de opsporingspraktijk laten

zien dat inkorten van de bewaartermijn voor de praktijk zeer onwenselijk is. De huidige bewaartermijnen worden door de opsporing en vervolging als adequaat (telefonie) of zelfs te kort (internet) ervaren.
Gegeven de privacy en terughoudendheid die daarbij hoort als reactie op de uitspraak van het Hof en de voorlichting van de Raad van State acht de regering harmonisering van de bewaartermijn, het gelijk trekken naar twaalf maanden voor zowel telefonie als internet, op dit moment niet opportuun. Daarom wordt in het conceptwetsvoorstel voorgesteld de bewaartermijnen onveranderd te laten. Dat wil zeggen, een bewaartermijn van zes maanden voor internetgegevens en twaalf maanden voor telefonie.

Vraag 24

Is een bewaarplicht van een half jaar voor alle gegevens, aangevuld met de mogelijkheid om gegevens te bevriezen als het vermoeden bestaat dat ze nog nodig zijn voor onderzoek, een alternatief?

Antwoord 24

Nee, het bevriezen van gegevens is geen vergelijkbaar en gelijkwaardig alternatief voor het opvragen van verkeersgegevens die voortkomen uit de bewaarplicht. In de huidige situatie is bevriezen van vluchtige gegevens op een zendmast al mogelijk op grond van artikel 126ni/ui van het Wetboek van Strafvordering. Dergelijke gegevens zijn echter maar enkele uren beschikbaar en kunnen dus alleen gevorderd worden als een delict snel ter kennis van de politie komt en het snel duidelijk is waar dat delict is gepleegd. Dit wordt ook bevestigd door de resultaten van het WODC onderzoek. Als historische gegevens maar zes maanden opgeslagen mogen worden gaat er veel, voor de opsporing zeer belangrijke, informatie verloren. In dit verband verwijs ik naar paragraaf 5.2 van de reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie waar een voorbeeld wordt genoemd van een kinderpornozaak die niet in behandeling kon worden genomen omdat de bewaartermijn van internetgegevens reeds verstreken was op het moment dat IP-adressen van mogelijke verdachten bekend werden. Zonder de historische internetgegevens zijn gebruikers van die IP-adressen niet meer te achterhalen.

Vraag 25

De leden van de PVV-fractie vragen in hoeveel gevallen de bewaartermijn van een jaar te kort blijkt te zijn om een opsporingsonderzoek goed te kunnen uitvoeren.

Antwoord 25

Ik beschik niet over concrete cijfers van opsporingsonderzoeken waarin de bewaartermijn van een jaar te kort bleek te zijn om een opsporingsonderzoek goed uit te kunnen voeren. Wel blijkt uit de praktijk – zo staat ook te lezen in het rapport van het WODC – dat bijvoorbeeld langlopende onderzoeken naar criminele organisaties, vermissingen, of anderszins, gebaat zouden kunnen zijn bij een langere bewaartermijn. In dergelijke gevallen kan pas na het verstrijken van de bewaartermijn blijken dat bepaalde gegevens relevant zijn, terwijl die gegevens op dat moment niet meer

beschikbaar zijn. Iets dergelijks kan ook voorkomen bij minder complexe onderzoeken. Een voorbeeld hiervan is de volgende zaak.
Nederland krijgt het verzoek van Zwitserland de afpersing, vrijheidsberoving en mishandeling van een Zwitsers staatsburger in Den Haag te onderzoeken en vervolgen. Tijdens het onderzoek blijkt dat verschillende in een Nederlands drugsonderzoek afgeluisterde telefoongesprekken gelieerd kunnen worden aan de afpersing van de Zwitser. Middels rechercheren op die afgetapte gesprekken kunnen alle afpersers geïdentificeerd worden op één na: die gebruikte een prepaid telefoon en werd nooit bij naam genoemd in de telefonische contacten. De historische verkeersgegevens van die prepaid telefoon konden niet meer worden opgevraagd voor de periode rondom de afpersing omdat de bewaartermijn reeds was verstreken. Zou dat wel hebben gekund, dan was de kans groot dat ook deze afperser geïdentificeerd zou zijn. Nu blijft hij buiten beeld (het betreffende telefoonnummer blijkt inmiddels van eigenaar gewisseld), terwijl zijn collega-afpersers worden veroordeeld tot gevangenisstraffen.

Vraag 26

De leden van de VVD-fractie lezen in het WODC-rapport dat aanbieders gegevens dienen te bewaren, op te slaan, te beveiligen, beschikbaar te stellen voor de opsporing en tijdig weer te vernietigen. Deze leden begrijpen dat dit kosten met zich meebrengt. Graag krijgen zij een nadere toelichting van de minister over de vergoeding van personele inzet voor grote aanbieders.

Antwoord 26

Op basis van de Telecommunicatiewet is met de zes grote telecomaanbieders een vergoedingsovereenkomst afgesloten.

Voor de kleine aanbieders geldt inzake de vergoeding van de gemaakte administratiekosten en personeelskosten die rechtstreeks voortvloeien uit het uitvoeren van aftap- of informatieverstrekkingsactiviteiten de Regeling kosten aftappen en gegevensverstrekking (Regeling van de Minister van Economische Zaken van 19 september 2014, nr. WJZ/14139301, tot wijziging van de Regeling kosten aftappen en gegevensverstrekking).

In de reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie wordt gewezen op de positie van de middelgrote en kleine aanbieders. 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 aan deze groep van aanbieders ruimte kan worden geboden om de naleving van de verplichtingen op een zo efficiënt mogelijke wijze vorm te geven. Met de aanbieders zal worden besproken welke praktische oplossingen denkbaar zijn om aan de naleving van de wettelijke verplichtingen te voldoen, waarbij onevenredige kosten en inspanningen waar mogelijk vermeden worden.

Vraag 27

Welke voorwaarden zijn aan een personele vergoeding verbonden?

Antwoord 27

De voorwaarden die aan een vergoeding zijn verbonden zijn terug te vinden in de Regeling kosten aftappen en gegevensverstrekking.

Vragen 29 en 30

Kan de minister tevens ingaan op de door het WODC genoemde technologische ontwikkelingen en de gevolgen van het 24/7 gebruik van de smartphone, de voortdurende connectie met het internet, het gebruik van WhatsApp, Hotmail, Gmail of Yahoo en het opslaan van bestanden in de cloud?
Dit alles brengt complicaties met zich mee voor het door Nederlandse opsporingsdiensten opvragen van verkeersgegevens van buitenlandse aanbieders. Welke gevolgen heeft dit voor de effectiviteit van de wet?

Antwoorden 29 en 30

Voor de opsporing is het natuurlijk altijd een uitdaging, maar ook van belang om technologische ontwikkelingen te volgen en daar, binnen de kaders die de wet stelt, zo goed mogelijk op in te spelen.
De technologische ontwikkelingen rondom internet en internetgerelateerde communicatie (waaronder) het 24/7 gebruik van de smartphone maakt dat de momenteel bewaarde verkeersgegevens van internetcommunicatie minder bruikbaar zijn dan ten tijde van het opstellen van de Richtlijn dataretentie en de Wet bewaarplicht werd gedacht. Naar aanleiding van het arrest van het Hof van Justitie en het WODC onderzoek heeft een evaluatie van de lijst van de te bewaren telecommunicatiegegevens plaatsgevonden. Daarbij is onderzocht welke gegevens strikt noodzakelijk zijn voor het voorkomen, opsporen of vervolgen van ernstige criminaliteit. Dit heeft geleid tot aanpassing en, waar nodig, verduidelijking van de lijst van te bewaren telecommunicatiegegevens.
De Wet bewaarplicht heeft gelet op het territorialiteitsbeginsel slechts betrekking op gegevens bij buitenlandse aanbieders, voor zover er verband is met het aanbieden van hun netwerk of diensten in Nederland. Voor de gevallen waarin dit verband er niet is, zal in nationale wetgeving geen oplossing gegeven kunnen worden.

Vraag 31

Wordt de effectiviteit niet juist minder in de loop der jaren, met het uitbreiden van technologische mogelijkheden?

Antwoord 31

Dat is niet per definitie het geval. Technologische ontwikkelingen bij de opsporing kunnen ook meer mogelijkheden bieden waardoor de effectiviteit van de wet juist wordt verhoogd.

Vraag 32

De leden van de D66-fractie constateren dat het aantal opgevraagde gesprekken wordt geregistreerd. Dit geldt echter niet voor het aantal politieonderzoeken of het aantal personen. Deze leden zijn verbaasd dat er geen kennis is over de effectiviteit van de verzameling aan gegevens (aantal politiezaken) ten opzichte van de inbreuk op de privacy. Kan de minister de Kamer deze gegevens doen toekomen?

Antwoord 32

Op grond van de in de Telecommunicatiewet geregelde bewaarplicht moeten gebruikers- en verkeersgegevens worden bewaard door de aanbieders. Het aantal bevragingen van gebruikers- en verkeersgegevens wordt geregistreerd. De bevragingen hebben dus geen betrekking op gesprekken. Op hoeveel politieonderzoeken of aantal personen deze bevragingen betrekking hebben wordt niet geregistreerd.

Zoals in het antwoord op vraag 5 is toegelicht zijn de gegevens die in het kader van de bewaarplicht worden bewaard onmisbaar en van groot belang voor de opsporing en vervolging van ernstige misdrijven.

Om een goede afweging te laten plaatsvinden tussen de belangen van de opsporing en de (privacy)belangen van de (potentiele) verdachte, gelden voor politie en openbaar ministerie strenge voorwaarden voor de toegang tot deze gegevens. In het Wetboek van Strafvordering (Sv.) is geregeld wie onder welke voorwaarden toegang heeft tot de opgeslagen telecom- en internetgegevens. De officier van justitie kan een vordering doen tot verstrekking van verkeersgegevens
(art. 126n en 126u Sv.) ingeval van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of bij een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd.

In het conceptwetsvoorstel wordt voorgesteld de toegang tot de bewaarde verkeers- en locatiegegevens afhankelijk te stellen van een voorafgaande rechterlijke toetsing, zodat kan worden verzekerd dat deze gegevens uitsluitend worden geraadpleegd in de gevallen waarin daartoe voldoende aanleiding bestaat. De rechterlijke toetsing zal worden gewaarborgd door middel van het wettelijke vereiste van een voorafgaande machtiging van de rechter-commissaris.

Vragen 33 en 34

Daaruit moet blijken hoeveel data worden opgeslagen en in hoeveel zaken de verzameling van gegevens tot een positief resultaat heeft geleid.

Zo niet, hoe kan de minister dan conclusies trekken over de effectiviteit?

Antwoorden 33 en 34

Telecommunicatiegegevens worden veelal gebruikt in combinatie met andere tactische en technische opsporingsinformatie. Het is daarom niet mogelijk om op basis van de bestaande gegevens in cijfers aan te geven in hoeverre het aantal opgehaalde gegevens heeft geleid tot een positief resultaat in een opsporingsonderzoek.

Wel blijkt uit de interviews in het WODC rapport dat deze gegevens een grote bijdrage

leveren aan de opsporing en dus effectief zijn voor de aanpak van criminaliteit.

De noodzaak van de bewaarplicht wordt ook bevestigd door de voorbeelden die vanuit de opsporingspraktijk zijn aangeleverd. In de memorie van toelichting bij het conceptwetsvoorstel zijn praktijkvoorbeelden opgenomen waaruit het belang van de in het kader van de bewaarplicht te bewaren gegevens blijkt.

Vraag 35

De leden van de D66-fractie lezen dat identificatie van gebruikers van IP-adressen gemakkelijk te omzeilen is door het gebruik van gemeenschappelijke hotspots. Deze leden concluderen hieruit dat de toegevoegde waarde van de database daalt, omdat juist de plegers van ernstige misdrijven gebruik zullen maken van deze mogelijkheid. Deelt de minister deze conclusie?

Antwoord 35

Nee, het opslaan van gegevens heeft wel degelijk toegevoegde waarde. Het blijft een belangrijk opsporingsmiddel zelfs als de wet (deels) wordt omzeild. Het Hof van Justitie heeft dit ook in haar arrest van 8 april jl onderschreven. Het Hof geeft aan dat de omstandigheid dat aan de richtlijn kan worden ontkomen door het gebruik van bepaalde communicatiewijzen, niet maakt dat de maatregel op zich volledig ongeschikt is om de nagestreefde doelstellingen te bereiken. Dataretentie an sich is volgens het Hof geschikt om het nagestreefde doel van de richtlijn te verwezenlijken (punt 50 van het arrest).

Vraag 36

De leden van de SP-fractie zijn voorstander van de uitvoering van een Privacy Impact Assessment (PIA) zodra voorstellen worden gedaan die de privacy mogelijk bedreigen. In dit geval moet een PIA slechts aan de orde zijn bij uitbreiding van de wettelijke bewaarplicht, maar niet wanneer de bewaarplicht wordt beperkt. Deelt de minister die mening?

Antwoord 36

Ik ben van mening dat gezien het belang van de bescherming van de privacy het in dit geval belangrijk is om vóór het wijzigen van de wet de gevolgen van die wijzigingen voor de privacy inzichtelijk te maken en dat het daarom nodig is een PIA uit te voeren. De impact op de privacy is niet alleen afhankelijk van de hoeveelheid aan gegevens die worden opgeslagen maar is vooral afhankelijk van welke gegevens opgeslagen worden en onder welke voorwaarden door wie toegang tot die gegevens kan worden verkregen.

Vraag 37

Wat is volgens de minister in dit geval concreet het nut van een PIA?

Antwoord 37

Zoals ik in mijn brief van 12 februari 2014 aan uw Kamer heb aangegeven vergt een

besluit over aanpassing van de huidige wet- en regelgeving een zorgvuldige afweging. Nu ten tijde van de totstandkoming van de Wet bewaarplicht telecommunicatiegegevens het PIA toetsmodel nog niet bestond en dus geen PIA is uitgevoerd, acht ik het mede in het licht van het arrest van het Hof van Justitie van belang dat de impact van de privacy voorafgaand aan de wijziging van de wet wordt onderzocht. De consultatieperiode van het conceptwetsvoorstel zal worden benut voor het uitvoeren van een PIA.

Vraag 38

Is het stellen en beantwoorden van de fundamentele vraag van nut, noodzaak en effectiviteit van de bewaarplicht niet veel belangrijker dan het uitvoeren van een PIA?

Antwoord 38

Alle aspecten moeten zorgvuldig meegenomen worden in de afweging bij de keuzes omtrent de invulling van de Wet bewaarplicht. Zowel het nut, de noodzaak en de effectiviteit van de bewaarplicht als de privacy zijn belangrijke aspecten.

Vragen 39 en 40

De leden van de PVV-fractie vragen welke maatregelen genomen worden om zo veel mogelijk te voorkomen dat hackers toegang kunnen krijgen tot opgeslagen telecommunicatiegegevens.

De leden van de D66-fractie lezen in het onderzoeksrapport dat het risico ontstaat dat hackers toegang krijgen tot de gegevens. Welke oplossing ziet de minister voor dit serieuze probleem?

Antwoorden 39 en 40

Voor alle aanbieders van openbare netwerken en diensten gelden verplichtingen ten aanzien van de borging van de integriteit en veiligheid van hun netwerken en diensten – zoals het waarborgen van de vertrouwelijkheid van communicatie (hoofdstuk 11 Tw). Daarnaast is het Besluit beveiliging gegevens aftappen telecommunicatie van toepassing. Dit besluit ziet toe op door aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten te treffen beveiligingsmaatregelen ten aanzien van gegevens betreffende het aftappen en opnemen van telecommunicatie. Het gaat onder meer om beveiligingseisen ten aanzien van personeel, fysieke beveiliging en beveiliging van de omgeving, toegangsbeveiliging van geautomatiseerde informatiesystemen, ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen.

Verder verwijs ik hier naar paragraaf 8 van de memorie van toelichting bij het conceptwetsvoorstel waarin het voornemen is opgenomen de gegevens die ten behoeve van de opsporing en vervolging worden opgeslagen beter af te schermen tegen inzage door onbevoegden. De regering zal onderzoeken of aangescherpte beveiliging door middel van versleuteling van deze gegevens kan plaatsvinden. Bij de consultatie van marktpartijen zal dit aspect eveneens aan de orde komen.

Vragen 41 en 42

Kan de minister voorts toelichten wie er toegang heeft tot welk stuk van de database?

Kan de minister tevens aangeven om welke redenen deze personen tot deze stukken van de database toegang hebben?

Antwoorden 41 en 42

Het Besluit beveiliging gegevens telecommunicatie (Bbgt) schrijft voor dat door de aanbieders beveiligingsmaatregelen moeten worden genomen. De dataretentie database heeft hierdoor een zeer beperkte toegang. Alleen medewerkers werkzaam bij de betreffende aanbieder die vanuit hun functie in aanraking komen met het behandelen van vorderingen van behoeftestellers hebben toegang. Deze taak is in hun functieomschrijving opgenomen met de daarbij behorende autorisatie. Deze medewerkers zijn in het bezit van een verklaring omtrent het gedrag (VOG).

Vragen 43 en 44

De leden van de D66-fractie lezen voorts dat voor kleine aanbieders de procedure anders verloopt en dat een medewerker handmatig gegevens uit het systeem haalt. Deelt de minister de opvatting dat een dergelijke werkwijze, negatieve gevolgen kan hebben voor de privacy van de klanten van deze kleine aanbieders?

En welke gevolgen verbindt de minister hieraan, ook gezien artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)?

Antwoorden 43 en 44

Nee. Het feit dat de kleine aanbieders gegevens handmatig uit het systeem halen, betekent niet dat dit negatieve gevolgen heeft voor de privacy. Het eerder genoemde Besluit beveiliging gegevens telecommunicatie (Bbgt) kent geen onderscheid tussen het geautomatiseerd zoeken of handmatig zoeken in de database om antwoord te kunnen geven op een vordering. Van kleine aanbieders kan niet verlangd worden om een geautomatiseerde zoekfunctie voor het beantwoorden van een vordering van behoeftestellers te installeren zoals dat bij de grote aanbieders die regelmatig bevraagd worden wel kan.

Vragen 45 en 46

De leden van de D66-fractie lezen in het onderzoeksrapport dat onderzoek gewenst is naar de opslag en vernietiging van de gegevens in verband met de privacy. Is de minister bereid hier onderzoek naar te doen?

Wanneer kan de Tweede Kamer de resultaten van dit onderzoek verwachten?

Antwoorden 45 en 46

In de ‘Meting dataretentie 2013’ wordt door het AT ingegaan op de naleving van de Wet

bewaarplicht telecomgegevens, waaronder het vernietigen van gegevens. Op 16 mei 2014 is de Kamer hierover bericht en is ingegaan op onder andere de naleving (en handhaving) van deze wettelijke bepalingen. Agentschap Telecom houdt voortdurend toezicht op deze eisen.

Vragen 47 en 48

De leden van de ChristenUnie-fractie vragen de minister of hij het inzicht deelt dat de potentiële inbreuk die de aan de wet gerelateerde bijzondere opsporingsbevoegdheden kunnen maken, de laatste jaren enorm is gegroeid. Is de minister bereid om de waarborgen voor deze opsporingsbevoegdheden om die reden te versterken?

Antwoorden 47 en 48

In het conceptwetsvoorstel worden extra waarborgen voorgesteld voor de toegang tot de gegevens met betrekking tot (internet)telefonie over een vast of mobiel netwerk ten behoeve van de opsporing van strafbare feiten. De toegang wordt beperkt aan de hand van de ernst van het betreffende misdrijf. De nadere regeling van de toegang komt op het volgende neer. De bewaartermijn is voor de gegevens met betrekking tot (internet)telefonie over een vast of mobiel netwerk vastgesteld op twaalf maanden. De bewaartermijn van twaalf maanden kan, anders dan tot nu toe, echter alleen volledig benut worden wanneer sprake is van de zwaarste categorie delicten, met een strafdreiging van acht jaar of meer. Bij lichtere delicten, waarvoor voorlopige hechtenis mogelijk is en waarop een maximale gevangenisstraf staat van minder dan 8 jaar, mogen de gegevens slechts gedurende een periode van zes maanden worden gevorderd. In het conceptwetsvoorstel wordt verder voorgesteld de toegang tot de bewaarde verkeers- en locatiegegevens afhankelijk te stellen van een voorafgaande rechterlijke toetsing, zodat kan worden verzekerd dat deze gegevens uitsluitend worden geraadpleegd in de gevallen waarin daartoe voldoende aanleiding bestaat. De rechterlijke toetsing zal worden gewaarborgd door middel van het wettelijke vereiste van een voorafgaande machtiging van de rechter-commissaris.

Vragen 49, 50 en 52

Er zijn signalen dat ook Nederland slechts zeer beperkt gegevens aanlevert. De leden van de PvdA-fractie vinden het van belang dat er goede gegevens zijn over het gebruik van deze richtlijn, zodat er ook zinvolle conclusies getrokken kunnen worden over het nut van de dataopslag. Welke gegevens levert Nederland aan de Europese Commissie?

Hoe vaak is dit gebeurd?

De leden van de ChristenUnie-fractie merken op dat Nederland op grond van de Richtlijn dataretentie verplicht is om elk jaar statistieken over de verwerkte gegevens aan de Europese Commissie te verstrekken. Kan de minister aangeven in hoeverre aan deze verplichting is voldaan?

Antwoorden 49, 50 en 52

Nederland heeft statistieken over het aantal verzoeken om gegevens over 2008 geleverd ten behoeve van de evaluatie van de richtlijn dataretentie door de Commissie. Met de

uitspraak van het Hof van Justitie waarin de richtlijn dataretentie met terugwerkende kracht ongeldig is verklaard is deze verplichting tot leveren van statistieken komen te vervallen.

Vragen 51 en 53

Ook vragen deze leden bij de Europese Commissie te bevorderen dat de statistieken van verschillende Europese lidstaten op elkaar aansluiten en regelmatig gepubliceerd worden.

Kan de minister deze statistieken vanaf nu ook openbaar maken?

Antwoorden 51 en 53

Nu de richtlijn ongeldig is verklaard, bestaat er ook geen verplichting meer tot het aanleveren van deze gegevens.

Vraag 54

De leden van de PvdA-fractie vinden de inhoudelijke evaluatie op Europees niveau van de Richtlijn dataretentie van belang. Op welke wijze wordt de richtlijn inhoudelijk geëvalueerd?

Antwoord 54

Voorafgaand aan de ongeldig verklaring van de richtlijn werd de richtlijn conform artikel 14 van die richtlijn door de Europese Commissie geëvalueerd. Deze evaluatie door de Commissie is neergelegd in een evaluatierapport van 18 april 2011 (kenmerk: COM(2011) 225 final). De Nederlandse inbreng bij de Europese Commissie ten behoeve van de evaluatie is op 20 december 2010 aan de Eerste Kamer (Kamerstukken 2010-2011, Kamerstuk 31145, nr. R) gestuurd.
Nederland heeft als eerste lidstaat een evaluatie van de nationale wetgeving aan de Commissie toegezonden.

Vraag 55

Welke wijzigingen wil de minister in deze richtlijn aangebracht zien?

Antwoord 55

Door het ongeldig verklaren van de richtlijn, is een wijziging niet langer aan de orde.

Vraag 61

Het opvragen van gebruikersgegevens kan een beperking op het recht op privacy zijn. In bepaalde gevallen is een dergelijke beperking toegestaan, namelijk wanneer dit bij wet voorzien is en noodzakelijk is in een democratische samenleving, aldus het EVRM. Hoe kan het dat er aanbieders zijn die geen gehoor geven aan de bewaarplicht van

verkeersgegevens vanuit idealistische standpunten?

Antwoord 61

In het WODC rapport wordt melding gemaakt van een kleine aanbieder van hostingdiensten die vanuit een idealistisch standpunt heeft aangegeven geen gegevens te willen bewaren. Los van de opvatting van de ondervraagde, is de kwestie dat een aanbieder van dergelijke hostingdiensten, geen aanbieder is in de zin van de Telecommunicatiewet. De bewaarplicht is daarom niet van toepassing op die dienstverlening.

Vraag 62

Graag krijgen zij een overzicht van de minister van de aanbieders die geen gegevens opslaan en zich niet conformeren aan de wet.

Antwoord 62

Uit het rapport "Meting dataretentie 2013" van het AT en de daarbij gevoegde brief aan de Tweede Kamer (Kamerstukken 2013-2014, 26 643, nr 313) over de naleving van de Wet bewaarplicht telecomgegevens is het beeld dat van de 343 geïnspecteerde aanbieders, 24 niet geheel voldoen aan de bewaarplicht. De groep van 343 aanbieders kan worden verdeeld in een groep van 6 grote aanbieders, die in totaal circa 98% van de bevragingen van opsporingsdiensten verzorgt, en een groep van 337 kleinere aanbieders waar ca. 2% van de bevragingen terecht komt. Uit informatie afkomstig uit reguliere toezichtactiviteiten in 2013 blijkt dat de 6 grote aanbieders voldoen aan de bewaarplicht.

Voor verdere informatie over naleving en het handhavingsbeleid van de Wet bewaarplicht telecomgegevens verwijs ik u naar de hiervoor genoemde Kamerstukken.

Vragen 63, 64, 65 en 66

De leden van de SP-fractie merken op dat het bij wet is vastgelegd dat aanbieders van telecom- en internetdiensten verkeersgegevens moeten bewaren. Deelt de minister de mening dat het niet bewaren van deze gegevens door bepaalde aanbieders ongewenst is en de opsporingstaken bemoeilijkt?

Deelt de minister voorts de mening dat dergelijke providers aantrekkelijk kunnen zijn voor personen uit het criminele milieu, aangezien zij weigeren aan hun wettelijke bewaarplicht te voldoen?

Is de minister het ermee eens dat de wet op deze manier minder doelmatig is?

Deelt de minister de mening dat het niet aan individuele bedrijven of burgers is om zich wel of niet aan de wet te willen houden of niet?

Antwoorden 63, 64, 65 en 66

Uiteraard is het ongewenst als bepaalde aanbieders telecommunicatiegegevens niet bewaren. Bij het beoordelen van de impact op de opsporing moet wel worden opgemerkt

dat ruim 90% van de markt in handen is van de grote zes aanbieders, die voldoen aan de bewaarplicht. Uit het rapport 'Meting dataretentie 2013' van het ministerie van EZ, dat op 16 mei 2014 aan uw Kamer is aangeboden, blijkt dat het aantal bevragingen van opsporingsdiensten bij de overige kleinere aanbieders relatief beperkt is en ca. 2% van het totaal aantal bevragingen omvat.
Dit neemt niet weg dat, zoals aan uw Kamer gemeld in voornoemde brief van 16 mei 2014, het AT de komende toezichtperiode zal inzetten op een verbetering in de naleving van deze verplichtingen. Het AT is daarbij bevoegd boetes op te leggen oplopend tot €450.000 per overtreding.

Vraag 67

Is de minister voornemens de wet te verduidelijken en techniekonafhankelijk te maken, zodat volkomen duidelijk is op welke gebruikersgegevens de wet van toepassing is en de wet niet meer achterhaald zal worden door technologische ontwikkelingen?

Antwoord 67

Het is nooit helemaal mogelijk om de wet techniekonafhankelijk te maken, zodat deze niet meer achterhaald kan worden door technologische ontwikkelingen. De onduidelijkheden voor de toepassing van de wet komen echter niet voort uit de afhankelijkheid van de techniek en de gevolgen van technologische ontwikkelingen. Voor zover er onduidelijkheid bestaat over welke gegevens bewaard moeten worden, volgt dit uit de formuleringen in de wet. Door bijvoorbeeld expliciet tot uitdrukking te brengen wat onder de term IP-adres moet worden verstaan en dat bepaalde vormen van internettelefonie tot telefonie via een vast of mobiel netwerk behoren, wordt deze onduidelijkheid weggenomen.

Vraag 68

Volgens de leden van de PvdA-fractie is het opvragen van eigen gegevens die opgeslagen worden in een informatiesysteem, een belangrijke manier om de correcte werking op individueel niveau aan te tonen en om zich ervan te verzekeren wat er precies met de eigen gegevens gebeurt. De ervaring van de onderzoekers en van meerdere journalisten bij het opvragen van de gegevens die telecomdienstverleners opslaan, is zeer negatief. De gegevens die geleverd worden, zijn verre van volledig en moeilijk te verkrijgen. Dat schokt deze leden, omdat hiermee belangrijke rechten niet uitgeoefend kunnen worden. Deelt de minister de mening dat de huidige informatievoorziening ook ver onder de maat is?

Antwoord 68

Uiteraard is het belangrijk dat de aanbieders uitvoering geven aan het in de Wet bescherming persoonsgegevens opgenomen recht op inzage van de eigen persoonsgegevens. Uit de jurisprudentie blijkt dat zelfs indien sprake zou zijn van een moeilijk toegankelijke gegevensverwerking, de inzage nog steeds verleend moet worden. Het is aan het CBP om in actie te komen als zij constateren dat de aanbieders in gebreke blijven.

Vraag 71

Naar de mening van de leden van de PvdA-fractie is de verhouding tussen het aantal keren dat gegevens zijn opgevraagd en deze daadwerkelijk zijn verstrekt, een interessant gegeven in de statistieken. Dit kan iets zeggen over de mate waarin de betrokken opsporingsdiensten in de praktijk inbreuk maken op de privacy van burgers. Daarom vragen deze leden of de statistieken over het gebruik van de wet met deze informatie uitgebreid kunnen worden.

Antwoord 71

Het proces rondom het bevragen bij en het verstrekken door de providers ziet er als volgt uit: De verzoeken om telecommunicatiegegevens van de opsporingsdiensten worden via de afdeling Interceptie & Sensing (I&S) Politie van de Landelijke Eenheid aan de providers toegezonden via een beveiligde verbinding.
Op die manier zijn de providers ervan verzekerd dat het om een gevalideerd verzoek gaat. Vervolgens wordt een query uitgevoerd op de database. Bij de grote zes providers vindt deze query geautomatiseerd plaats, bij de kleinere providers gebeurt dit veelal handmatig. Vervolgens wordt een bestand gecreëerd waarin de gevraagde gegevens worden opgenomen. Dit bestand wordt weer via een beveiligde verbinding aan I&S toegezonden.

Op het verwerken en beantwoorden van een verzoek om persoonsgegevens zijn beveiligingsmaatregelen van toepassing. Deze regels zijn neergelegd in het Besluit beveiliging gegevens telecommunicatie. Het AT ziet toe op de naleving van deze regels. Zo moeten de gegevens die de aanbieders sinds 2009 moeten bewaren, worden opgeslagen in een eigen database die in een beveiligde omgeving staat en mogen deze gegevens slechts voor een select aantal medewerkers van de aanbieder benaderbaar zijn.

Statistieken over de verhouding tussen het aantal keren dat gegevens zijn opgevraagd en daadwerkelijk zijn verstrekt worden niet bijgehouden en kunnen dus niet worden verstrekt.

Vraag 72 en 73
Ook willen zij weten of de statistieken in Nederland en in andere Europese lidstaten opgesteld kunnen worden volgens de richtlijnen van het Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime.
Zo ja, hoe snel kan de overheid gebruikmaken van deze richtlijn?

Antwoorden 72 en 73

Deze richtlijnen zijn opgesteld op basis van de richtlijn dataretentie. Gelet op de ongeldigverklaring van de richtlijn is het aanleveren van statistieken aan de Europese Commissie nu niet aan de orde.

Vraag 76

De leden van de D66-fractie lezen in de reactie van het College bescherming

persoonsgegevens (CBP), Bits of Freedom en het Rathenau Instituut dat klanten geen recht tot inzage hebben in hun verkeers- en locatiegegevens en dat daarom niemand zicht heeft of de verwerking van de gegevens wel rechtmatig en correct gebeurt. Wat betekent dit gegeven voor de notificatieplicht?

Antwoord 76

De notificatieplicht is aan de orde als gebruik is gemaakt van strafvorderlijke bevoegdheden om gebruikersgegevens te vergaren. Dat houdt in dat de officier van justitie aan de betrokkene van wie gegevens zijn opgevraagd, mededeling moet doen zodra het belang van het onderzoek dit toelaat. De verantwoordelijkheid voor de notificatieplicht ligt dus bij de officier van justitie en staat los van het recht op inzage van de eigen verkeers- en locatiegegevens die opgeslagen liggen bij de providers. Voor het verstrekken van inzage in de opgeslagen gegevens zijn de providers verantwoordelijk.

Vraag 78

De leden van de PVV-fractie vragen of de minister maatregelen kan nemen om er in het kader van de opsporingspraktijk zorg voor te dragen dat uit de opgevraagde gegevens naast de startlocatie van een gesprek ook de eindlocatie opgemaakt kan worden.

Antwoord 78

Uit het WODC onderzoek blijkt dat er behoefte bestaat aan de opslag van de zogenaamde last cell (eindlocatie) gegevens. De beginlocatie, dat is de mast die wordt aangestraald aan het begin van een gesprek, valt onder de bewaarplicht. Echter, waar het gesprek eindigt – dus de laatste connectie met een zendmast – valt niet onder de bewaarplicht.
Dit betekent dat wanneer iemand bellend de auto of trein instapt, uit de historische verkeersgegevens niet valt op te maken op welke locatie het gesprek eindigt. Door de eindlocatie van een gesprek op te slaan kan gerichter worden gezocht naar verdachten of getuigen, omdat aan de hand van de masten die zijn aangestraald tijdens het begin van het gesprek en het einde van het gesprek inzichtelijk is in welk gebied zij zich bevonden. Ook kunnen personen uitgesloten worden als verdachte omdat uit de eindlocatie van het gesprek dat zij gevoerd hebben blijkt dat zij ten tijde van het delict niet (meer) in de buurt waren. De eindlocatiegegevens zijn dus erg waardevol voor opsporingsonderzoeken.
Echter, gelet op de privacy en terughoudendheid die daarbij hoort als reactie op de uitspraak van het Hof en de voorlichting van de Raad van State acht de regering het op dit moment niet opportuun de lijst van te bewaren gegevens uit te breiden met de eindlocatie van een gesprek.

Vragen 79, 82 en 83

De leden van de VVD-fractie lezen in het WODC-rapport dat de opgeslagen gegevens automatisch door bedrijven worden vernietigd na het verstrijken van de bewaartermijn. Hoe ziet het AT erop toe dat dit daadwerkelijk plaatsvindt?

De leden van de PvdA-fractie merken op dat de bewaarde gegevens na afloop van de

bewaartermijn vernietigd behoren te worden. Over de vraag of dit volledig en onmiddellijk gebeurt, valt weinig zekerheid te geven. Daarom vragen deze leden welke waarborgen er zijn dat gegevens die niet langer bewaard hoeven te worden, vernietigd worden.

Hoe is de afgelopen jaren toezicht gehouden op de vernietiging?

Antwoorden 79, 82 en 83

De geautomatiseerde vernietiging van opgeslagen gegevens vindt plaats door het uitvoeren van zogenaamde scripts. Deze scripts vernietigen dagelijks de opgeslagen gegevens die ouder zijn dan de verplichte bewaartermijn. Van het uitvoeren van deze scripts worden logfiles gecreëerd en opgeslagen. Het toezicht dat AT uitoefent op de beveiliging en vernietiging van gegevens die nodig zijn voor de opsporing bestaat op dit moment uit systeemtoezicht. Dat wil zeggen dat de toezichthouders van AT aan de hand van een beschrijving die de aanbieder geeft van zijn bedrijfsvoeringsprocessen en gehanteerde scripts, beoordelen of die aanbieder voldoende maatregelen heeft genomen om de beveiliging en vernietiging van deze gegevens te waarborgen.

Het AT is op dit moment niet gerechtigd om in de database zelf een controle uit te voeren of de desbetreffende data vernietigd is door de beperking in artikel 18.7, tweede lid, van de Tw. Daardoor kan niet feitelijk gecontroleerd worden of bijvoorbeeld de gegevens tijdig zijn vernietigd. Volgens het WODC mist AT hiermee een instrument om dit aspect van het toezicht goed uit te oefenen.

Gelet hierop wordt voorgesteld de tekst van artikel 18.7, tweede lid van de Telecommunicatiewet te wijzigen, om de toezichthouders van AT in staat te stellen om gegevens feitelijk in te zien.

Vragen 80 en 81

Daarnaast vragen de leden van de VVD-fractie hoe opsporings- en veiligheidsdiensten omgaan met het vernietigen van gegevens. Deze leden kunnen zich voorstellen dat opgevraagde gegevens die niet relevant blijken voor het betreffende onderzoek snel worden vernietigd. Graag een reactie van de minister hieromtrent.

Op welke manier kan toezicht hierop plaatsvinden?

Antwoord 80 en 81

Opgevraagde gegevens die niet relevant blijken voor het betreffende onderzoek moeten op grond van de Wet bescherming persoonsgegevens onmiddellijk worden vernietigd.

Het CBP houdt toezicht op naleving van de Wet bescherming persoonsgegevens.

Vragen 84 en 85

De leden van de VVD-fractie lezen in de brief van de minister dat hij de komende maanden zal verkennen in hoeverre de informatie uit het onderzoek aanleiding geeft de lijst met te bewaren gegevens die is opgenomen in de bijlagen van de Tw uit te breiden. Op welke extra te bewaren gegevens doelt de minister?

Vallen hier bijvoorbeeld de gegevens van de last cell (de eindlocatie) onder?

Antwoorden 84 en 85

Naar aanleiding van het arrest van het Hof van Justitie en het WODC onderzoek heeft een evaluatie van de lijst van de te bewaren telecommunicatiegegevens plaatsgevonden. Daarbij is onderzocht welke gegevens strikt noodzakelijk zijn voor het voorkomen, opsporen of vervolgen van ernstige criminaliteit. Dit heeft geleid tot aanpassing van de lijst van te bewaren telecommunicatiegegevens. Voorgesteld wordt onder meer om over te gaan tot schrapping van de gegevens met betrekking tot e-mail over internet, de datum en tijdstip van de log-in en log-off van een internetsessie gebaseerd op een bepaalde tijdzone samen met het IP-adres en de verplichting tot bewaring van locatiegegevens, anders dan de locatieaanduiding bij het begin van de verbinding (de zogenaamde first Cell ID). Voorgesteld wordt om de formulering van IP-adres aan te passen zodat IP-adressen, in lijn met de bedoeling van de bewaarplicht, te relateren zijn aan een gebruiker of abonnee.
De last cell gegevens worden niet toegevoegd aan de lijst met de te bewaren gegevens.

Vragen 87 en 88

De leden van de VVD-fractie hebben vragen over de effectiviteit van de wet. Zo is het merendeel van de gegevens betreffende internet zoals beschreven in de bijlage behorende bij artikel 13.2a Tw volgens experts verouderd. De regeling zou niet meer passen bij het huidige internetgebruik en bij de technologische ontwikkelingen die zich hebben voorgedaan sinds de invoering van de wet in 2009. De voornoemde leden delen de mening van de onderzoekers van het WODC dat hierdoor een situatie is ontstaan waarin gegevens van burgers worden bewaard die niet of nauwelijks worden gebruikt door opsporingsdiensten. Deelt de minister de mening dat een zorgvuldige heroverweging over het type te bewaren gegevens op zijn plek is?

Zo ja, gaat de minister hiermee aan de slag? Zo nee, waarom niet?

Antwoorden 87 en 88

Ja, ik deel deze mening. Daarom heeft een evaluatie van de lijst van de te bewaren telecommunicatiegegevens plaatsgevonden en wordt in het conceptwetsvoorstel voorgesteld om de lijst van te bewaren gegevens aan te passen.

Vragen 89 en 90

Daarnaast zijn deze leden van mening dat gegevens die nu juist wél nuttig zijn voor opsporingsdoeleinden niet onder de wet vallen, zoals Voice over Broadband (VoBB), Skype en Facetime. Deze leden achten het wenselijk dat ook deze gegevens gebruikt kunnen worden voor opsporingsdoeleinden, onder andere omdat er misdrijven zijn die online plaatsvinden, zoals de facilitering van terrorisme, online afpersing, phishing en digitale ontucht met minderjarigen (grooming). Zij zien graag een plicht tot het bewaren van gegevens voor deze aanbieders. Deelt de minister deze wens?
Zo ja, hoe zal dit gerealiseerd kunnen worden?

Antwoorden 89 en 90

Ik begrijp uw vraag aldus dat u de reikwijdte van "aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten" wilt uitbreiden met diensten als Skype en Facetime die nu niet onder die definitie vallen.
Op dit moment acht ik een dergelijke vergaande uitbreiding van de bewaarplicht, gelet op de privacy en terughoudendheid die daarbij hoort als reactie op het arrest van het Hof van Justitie, niet wenselijk nu dit een wezenlijke wijziging van de bewaarplicht zou betekenen.
Daar komt bij dat er ook de optie is om via een rechtshulpverzoek deze gegevens in het buitenland op te vragen zoals is beschreven in het antwoord op vraag 109.

Vragen 91 tot en met 101, 114

De leden van de PvdA-fractie lezen in de evaluatie dat de gegevens over het internetverkeer nauwelijks gebruikt worden en ook slecht bruikbaar zijn. De keus om deze gegevens dus niet meer op te slaan, ondersteunen deze leden van harte. De minister lijkt echter te suggereren andere gegevens die nu nog niet worden opgeslagen, wel op te willen slaan. Deze keus bevreemdt deze leden. Zij zien geen grond in de voorliggende evaluatie om het aantal opgeslagen gegevens te vergroten. Daarom horen zij graag hoe een eventuele uitbreiding van gegevens aansluit op de evaluatie.
Ook horen deze leden graag welke nieuwe gegevens opgeslagen zouden moeten worden.

Wat is de noodzaak van de generieke opslag van nieuwe gegevens?

Welke impact heeft dit naar verwachting van de minister op de privacy?

De leden van de SP-fractie constateren dat de minister gaat verkennen in hoeverre de informatie uit het onderzoek aanleiding geeft om de lijst met te bewaren gegevens die is opgenomen in de bijlage van de Tw, uit te breiden. Moet daar niet bij staan 'of te beperken'?

Of staat voor de minister op voorhand vast dat slechts naar uitbreiding gekeken moet worden? Zo ja, waarom?

De leden van de D66-fractie lezen in de evaluatie dat er weinig noodzaak is tot het uitbreiden van het aantal verzamelde gegevens, maar in de brief van de minister lezen zij een aankondiging tot verkenning van het bewaren van meer gegevens. Deze leden horen graag hoe dit samenhangt, welke argumenten er zijn voor het verzamelen van meer gegevens en waar dit blijkt uit het onderzoek. Graag ontvangen voornoemde leden paginanummers en citaten uit het onderzoek op basis waarvan de minister deze conclusie trekt.

Zij lezen dat het verzamelen van meer gegevens tot meer ruis kan leiden en efficiënte opsporing kan bemoeilijken. Kan de minister inhoudelijk ingaan op dit probleem?

Ziet de minister dit als een argument voor het verkleinen van de hoeveelheid gegevens?

De leden van de D66-fractie lezen dat door de regelgeving gegevens worden opgeslagen die door de opsporingsdiensten nooit worden geraadpleegd. Deze leden noemen hier de

gegevens betreffende internetverkeer opgenomen in artikel 13.2a Tw. Ziet de minister hier aanleiding in tot aanpassing van de wet? Zo nee, waarom niet?

Tot welke keuzes ten aanzien van verplichte databewaring leidt de voorkeur voor privacy by design?

Antwoorden 91 tot en met 101, 114

Naar aanleiding van het arrest van het Hof van Justitie en het WODC onderzoek heeft een evaluatie van de lijst van de te bewaren telecommunicatiegegevens plaatsgevonden. Daarbij is onderzocht welke gegevens strikt noodzakelijk zijn voor het voorkomen, opsporen of vervolgen van ernstige criminaliteit. Dit heeft geleid tot aanpassing van de lijst van te bewaren telecommunicatiegegevens. Ik verwijs in dit verband ook naar de beantwoording van de vragen 84 en 85.

Vraag 102

De leden van de ChristenUnie-fractie merken op dat de minister in zijn aanbiedingsbrief lijkt aan te sturen op verruiming van de bewaarplicht. Overweegt hij ook om de bewaarplicht op onderdelen juist in te perken, gezien het feit dat driekwart van de door het WODC onderzochte gegevens die zijn opgevraagd, zelfs niet ouder dan zes maanden is?

Antwoord 102

De evaluatie van de lijst van de te bewaren telecommunicatiegegevens heeft geleid tot aanpassing van die lijst. Een aantal gegevens wordt geschrapt van de lijst van te bewaren gegevens en een aantal formuleringen wordt verduidelijkt.
Voorgesteld wordt om de bewaartermijnen onveranderd te laten.
Verder wordt de toegang tot telefoniegegevens beperkt voor delicten met een strafbedreiging van minder dan 8 jaar.

Vraag 103

Hoe weegt de minister dat gegeven?

Antwoord 103

Uit het WODC onderzoek blijkt dat van de in 2012 in totaal 41.658 bevragingen van historische telecommunicatie gegevens ruim 11.000 van de bevraagde gegevens ouder waren dan 6 maanden. Het gaat dus om een kwart van de bevragingen en niet om een gering deel. Deze gegevens zijn vooral noodzakelijk in zware en vaak ingewikkelde zaken, zoals kinderporno of georganiseerde criminaliteit.

Vragen 104, 105 en 106

De leden van de VVD-fractie vragen welke maatregelen de minister gaat nemen om professionals uit de opsporingspraktijk meer kennis te laten verwerven over de wijze waarop historische gegevens betreffende het internetverkeer gebruikt kunnen worden

bij de opsporing. Uit de evaluatie blijkt dat de professionals niet voldoende kennis hebben.

De leden van de D66-fractie lezen in het onderzoeksrapport dat het de opsporingsambtenaren ontbreekt aan kennis over de digitalisering van de samenleving en dat dit gevolgen heeft voor de opsporing. Heeft dit volgens de minister gevolgen voor het nut en de noodzaak van het bewaren van de gegevens?

Zal de minister hiertegen stappen ondernemen, aangezien het onderzoeksrapport stelt dat het de effectiviteit van de opsporingsmethoden vermindert?

Antwoorden 104, 105 en 106

In het inrichtingsplan voor de nationale politie is specifiek expertise ingericht voor het digitale domein. Binnen de teams opsporing is voorzien in operationeel specialisten, senioren en generalisten opgeleid voor en
belast met het werkterrein digitale expertise. Hiermee wordt
bewerkstelligd dat in elk opsporingsonderzoek de mogelijkheden van digitaal opsporen worden onderkend en benut. Aanvullend is meer gespecialiseerde capaciteit beschikbaar vanuit het team Digitale Opsporing bij de Dienst Regionale Recherche. Het Team High Tech Crime van de Landelijke Eenheid is de afgelopen jaren fors uitgebreid en zal eind 2014 119 fte bevatten.
Binnen alle politieprocessen (zoals intake en handhaving) is door middel van de landelijke beleidsdoelstelling voor cybercrime de afgelopen jaren ingezet op versterking van de aanpak van cybercrime door het Team High Tech Crime. De Veiligheidsagenda 2015-2018 zet in op verdere versterking van de digitale expertise van de regionale eenheden. Dit gebeurt onder meer door middel van opleidingen.
De conclusie in het rapport ziet op kennis in de breedte. Zoals hierboven geschetst wordt deze kennis de komende jaren verder versterkt. In de diepte is die kennis er wel degelijk, zoals bijvoorbeeld bij Team High Tech Crime. Het is zaak dat deze kennis verder wordt verspreid onder de opsporingsdiensten.

Vragen 107 en 108

De leden van de ChristenUnie-fractie vinden de constatering zorgelijk dat professionals uit de opsporingspraktijk weinig tot geen kennis hebben over de wijze waarop historische gegevens betreffende het internetverkeer gebruikt kunnen worden in de opsporing. Ook vinden zij het zorgelijk dat zij de technologische ontwikkelingen nauwelijks bij kunnen houden. Nu er zo weinig gebruik van wordt gemaakt, lijkt het deze leden nuttiger dat wordt bekeken hoe de toepassing kan worden verbeterd dan te spreken over nog ruimere bevoegdheden.
Ook is het de vraag of, nu de gegevens weinig worden gebruikt, het aantal gegevens dat wordt bewaard niet beperkt moet worden.

Antwoorden 107 en 108

Dat er van historische gegevens voor internetverkeer minder gebruik wordt gemaakt dan van telefoongegevens heeft vooral te maken met het feit dat een deel van de bewaarde gegevens minder bruikbaar zijn als gevolg van technologische ontwikkelingen. Daarom wordt een aanpassing van de lijst van te bewaren telecommunicatiegegevens voorgesteld die zich beperkt tot gegevens die strikt noodzakelijk zijn voor het

voorkomen, opsporen of vervolgen van ernstige criminaliteit.
Uiteraard is het ook zaak, zoals bij het antwoord op vragen 104 t/m 106 is aangegeven, de aanwezige kennis binnen de opsporingsdiensten in de breedte uit te breiden.

Vraag 109

De leden van de VVD-fractie lezen in de evaluatie dat veel in Nederland gegenereerde gegevens niet onder de Nederlandse wet vallen, omdat de gebruikers een dienst afnemen bij Amerikaanse bedrijven zoals Hotmail, Yahoo, Google en Facebook. Deze leden willen graag van de minister weten hoe de samenwerking met dit soort bedrijven verloopt indien er een verzoek tot verstrekking van gegevens wordt gedaan.

Antwoord 109

Wanneer het openbaar ministerie gegevens wil vorderen van bedrijven die hun juridische vertegenwoordiging in het buitenland hebben (zoals Facebook of Google), dan verloopt de verkrijging van dergelijke gegevens in samenspraak met de daartoe aangewezen autoriteiten van het land alwaar het bedrijf juridisch gevestigd is. Het openbaar ministerie dient een rechtshulpverzoek in bij de buitenlandse autoriteit, waarna het verzoek conform de aldaar geldende regelgeving wordt behandeld. In sommige gevallen kan sprake zijn van een rechtstreekse bevraging bij de Amerikaanse aanbieder wanneer de Amerikaanse regelgeving dit toestaat. Voorts dient het verzoek te voldoen aan de vereisten voor de Nederlandse regelgeving voor het vorderen van gegevens, zoals neergelegd in onder andere titel IVa van het Wetboek van Strafvordering. Een dergelijk verzoek wordt derhalve alleen gedaan wanneer voldaan is aan de daarin opgenomen voorwaarden en de vereisten van proportionaliteit en subsidiariteit.

Vragen 110 en 111

Deelt de minister hun mening dat het wenselijk is de gegevens van Nederlandse gebruikers onder de Nederlandse wet te laten vallen?
Is het nodig de wet aan te passen zodat deze gegevens onder de Nederlandse wet vallen?

Antwoorden 110 en 111

Zoals ik in mijn antwoord op vragen 89 en 90 al heb aangegeven acht ik een dergelijke wijziging van de wet op dit moment niet opportuun.

Vraag 112

Hoe worden gegevens die zich op Nederlands grondgebied bevinden gevorderd en welke garanties biedt de Nederlandse wet ten opzichte van vorderingen gedaan vanuit het buitenland?

Antwoord 112

Wanneer buitenlande opsporingsdiensten gegevens willen vorderen die zich in Nederland bevinden, dan dienen zij daartoe een rechtshulpverzoek in. Indien aan de formele

vereisten voor het rechtshulpverzoek is voldaan, dan neemt het openbaar ministerie het verzoek in behandeling. Voor de verdere uitvoering gelden de voorwaarden die voor een "Nederlandse" vordering gelden onverkort: het opvragen van de gegevens dient proportioneel en subsidiair te zijn en te voldoen aan de eisen zoals deze zijn neergelegd in de artikelen 126n/u en 126na/ua van het Wetboek van Strafvordering.

Vragen 113, 115, 116 en 117

De leden van de PvdA-fractie hebben met grote instemming kunnen constateren dat de minister inzet op privacy by design, het uitgangspunt dat informatiesystemen zodanig ingericht worden dat de privacy maximaal gediend wordt. In dat kader vragen deze leden of er een alternatief is voor generieke dataopslag, zoals bij deze wet. Een alternatief is gerichte bevriezing van gegevens.

Ziet de minister ook voordelen in gerichte bevriezing?

De leden van de SP-fractie vragen een reactie op de suggestie die door o.a. Bits of Freedom is gedaan om te gaan werken met gerichte bevriezing als instrument om historische verkeersgegevens te bewaren. Dan worden gegevens alleen bewaard indien de politie hiertoe verzoekt, zodat niet langer alle verkeersgegevens van iedereen bewaard hoeven te worden.

De leden van de D66-fractie lezen dat er een mogelijkheid is tot het bevriezen van de gegevens als meer privacybestendige oplossing. Heeft de minister deze mogelijkheid verkend en overwogen?

Antwoorden 113, 115, 116 en 117

Het bevriezen van gegevens is geen alternatief voor de bewaarplicht. Bij bevriezing van gegevens stel je slechts zeker dat de op het moment van bevriezing beschikbare telecommunicatiegegevens beschikbaar blijven.
Het bevriezen van gegevens is zelfs niet altijd mogelijk, omdat gegevens soms al vernietigd zijn voor een bevel tot bevriezing is gegeven. Bevriezing van gegevens is alleen nuttig in gevallen waarin voor de politie snel duidelijk is dat er een delict gepleegd is en waar dat heeft plaatsgevonden. In andere situaties biedt het bevriezen van gegevens geen oplossing. In de meeste gevallen wordt een delict pas later bekend. Dan moet teruggekeken kunnen worden.
De Europese Commissie heeft ook onderzocht hoe bevriezing is toegepast in en buiten de EU en hoe effectief het is gebleken in strafrechtelijke onderzoeken.[1] Daarin wordt geconcludeerd dat de opslag van gegevens en het bevriezen van gegevens aanvullende instrumenten zijn en geen alternatieven van elkaar.

De opslag van historische gegevens en de bevriezing van gegevens hebben een verschillende functie en kunnen elkaar wel aanvullen maar niet vervangen. Met de eerste wordt naar het verleden gekeken, met het tweede in het heden. Aan gerichte

[1] Evidence of potential impacts of options for revising the data retention directive: Current approaches to data preservation in the EU and in third countries" van november 2012. (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf)

bevriezing kleven echter risico's. Om gericht te kunnen bevriezen zouden risicoprofielen moeten worden gemaakt van potentiele verdachten, zonder dat daarvoor een specifieke aanleiding is. Dat vind ik onwenselijk.

Vraag 118

Welke andere opties zijn verkend?

Antwoord 118

Er zijn geen andere opties voorhanden waarmee hetzelfde resultaat bereikt kan worden als met het opslaan van telecommunicatiegegevens.

Vragen 119 en 120

De leden van de ChristenUnie-fractie merken op dat verschillende organisaties de gerichte bevriezing als instrument om historische verkeersgegevens te bewaren, bepleiten. Bij een gerichte bevriezing worden gegevens pas opgeslagen door een provider als de politie hiertoe verzoekt in het kader van een opsporingsonderzoek. In het rapport van het WODC wordt opgemerkt dat dit geen vergelijkbaar of gelijkwaardig alternatief zou zijn voor de bewaarplicht. De voornoemde leden erkennen dat, maar zij missen een beoordeling op basis van proportionaliteit. Immers deze methode betekent wel een grotere bescherming van de privacy. In hoeverre brengt dit alternatieve instrument voldoende op voor de opsporingspraktijk in vergelijking tot de algehele bewaarplicht?
Waarom is dit niet nader onderzocht?

Antwoorden 119 en 120

Zoals de leden van de ChristenUnie zelf erkennen en bij de antwoorden op de vragen 113, 115, 116 en 117 is aangegeven, is bevriezing van gegevens geen alternatief voor de opslag van historische gegevens.
De twee opsporingsmiddelen dienen verschillende doelen.

Vragen 121 en 122

In 2012 zijn er 56.825 vorderingen gedaan tot verstrekking van verkeersgegevens. Echter, de onderzoekers van het WODC geven aan dat hier ook gegevens bij zitten die niet onder de bewaarplicht voor telecommunicatie vallen. Deze leden zijn van mening dat de door de minister verstrekte gegevens geen duidelijkheid geven over het aantal personen van wie de gegevens zijn opgevraagd en ook niet over de vraag of de vordering daadwerkelijk tot een verstrekking van gegevens heeft geleid.
Kan de minister in de toekomst transparantere en betekenisvollere gegevens over het aantal bevragingen publiceren?
Welke rol is voor het AT weggelegd met betrekking tot het transparanter en inzichtelijker maken van vorderingen en verstrekte gegevens?

Antwoorden 121 en 122

Het is de rol van de overheid om cijfers te publiceren. Publicatie van deze cijfers vindt

plaats in het jaarverslag van het ministerie van Veiligheid en Justitie.

De aard van de verzoeken en de wijze waarop deze worden geregistreerd maken het niet mogelijk om inzicht te geven in de hoeveelheid politieonderzoeken of het aantal personen waarop bevraagd wordt.