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

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het noodzakelijk is het Wetboek van Strafvordering en de Telecommunicatiewet te wijzigen in verband met de ongeldigverklaring van Richtlijn nr 2006/24/EG van het Europees Parlement door het Hof van Justitie van de Europese Unie en de wenselijkheid van een nationale verplichting betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel I

De Telecommunicatiewet wordt als volgt gewijzigd:

A

Artikel 13.2a, tweede lid, komt te luiden:

2. Aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten bewaren de in de bij deze wet behorende bijlage aangewezen gegevens, voor zover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, teneinde te kunnen voldoen aan een vordering op grond van artikel 126n, artikel 126u of artikel 126zh van het Wetboek van Strafvordering.

B

Artikel 13.4 wordt als volgt gewijzigd:

1. In het eerste lid wordt de zinsnede 'artikel 126n of artikel 126na, dan wel artikel 126u of artikel 126ua' vervangen door: 'artikel 126n, eerste lid, 126u, eerste lid, of 126zh'.

2. In het derde lid vervalt de tweede volzin.

C

Artikel 13.5, derde lid, wordt als volgt gewijzigd:

Onder vervanging van de punt aan het slot van onderdeel b door een puntkomma wordt een onderdeel toegevoegd, luidende:

c. worden opgeslagen en verwerkt in Nederland of in een andere lidstaat van de Europese Unie.

D

Artikel 13.9 komt te luiden:

Artikel 13.9
Onze Minister van Veiligheid en Justitie zendt in overeenstemming met Onze Minister binnen drie jaar na de inwerkingtreding van deze wet en vervolgens telkens na drie jaar aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van deze wet in de praktijk.

E

Artikel 18.7, tweede lid, komt te luiden:

2. De bevoegdheid, bedoeld in het eerste lid, strekt zich met betrekking tot verkeers- en locatiegegevens slechts uit tot de gegevens die op grond van artikel 13.2a worden bewaard, voor zover dit nodig is voor het toezicht op de naleving van het bepaalde bij of krachtens hoofdstuk 13.

F

De bijlage behorende bij artikel 13.2a van de Telecommunicatiewet wordt als volgt gewijzigd:

1. In het eerste onderdeel a vervalt: , enhanced media service (EMS) en multimedia service (MMS).
2. Aan onderdeel A wordt na "Bij" ingevoegd: (internet).
3. In onderdeel B vervalt: , e-mail over het internet en internettelefonie.
4. In onderdeel B vervallen de onderdelen a, e, g en h, onder verlettering van de onderdelen b, c, d en f tot a, b, c respectievelijk d.
5. In onderdeel B komt onderdeel c (nieuw) te luiden:
c. De IP-adressen (inclusief datum en tijdstip), hetzij statisch, hetzij dynamisch, die door de aanbieder van een internettoegangsdienst aan een communicatie zijn

toegewezen, de gebruikersidentificatie van de abonnee of geregistreerde gebruiker, alsmede het poortnummer voor zover dit nodig is om de gebruiker te identificeren.

Artikel II

Het Wetboek van Strafvordering wordt als volgt gewijzigd:

A

Artikel 126n wordt als volgt gewijzigd:

1. Onder vernummering van het derde tot en met zesde lid tot respectievelijk het zesde tot en met negende lid, worden drie leden ingevoegd, die komen te luiden:

3. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder *a*, die door een aanbieder worden bewaard op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet, kan de vordering slechts betreffen:
a. ingeval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid; de gegevens, bedoeld in artikel 13.2a, derde lid, onderdelen a en b, van de Telecommunicatiewet, die door de aanbieder van een communicatiedienst zijn vastgelegd gedurende een periode van zes maanden voorafgaand aan de datum van de vordering;
b. ingeval van verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld; de gegevens, bedoeld in artikel 13.2a, derde lid, onderdeel a, van de Telecommunicatiewet, die door de aanbieder van een communicatiedienst zijn vastgelegd gedurende een periode van twaalf maanden voorafgaand aan de datum van de vordering;
4. Een vordering als bedoeld in het derde lid kan slechts worden gedaan na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 126*l*, zevende lid, is van overeenkomstige toepassing.
5. Een vordering als bedoeld in het derde lid is schriftelijk en vermeldt:
a. indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon over wie gegevens worden gevorderd;
b. (een zo nauwkeurig mogelijke aanduiding van) de gegevens die worden gevorderd;
c. de periode waarover de vordering zich uitstrekt.

2. In het zevende lid (nieuw) wordt, onder vernummering van onderdeel e tot onderdeel f, een onderdeel e ingevoegd, luidende:

e. indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder *a*, de periode waarover de vordering zich uitstrekt;

B

Artikel 126u wordt als volgt gewijzigd:

1. Onder vernummering van het derde tot en met het zesde lid tot respectievelijk het zesde tot en met het negende lid, worden drie leden ingevoegd, luidende:

3. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder *a*, die door een aanbieder worden bewaard op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet, kan de vordering slechts betreffen:
a. ingeval van een redelijk vermoeden dat een misdrijf wordt beraamd of gepleegd als omschreven in artikel 67, eerste lid; de gegevens, bedoeld in artikel 13.2a, derde lid, onderdelen a en b, van de Telecommunicatiewet, die door de aanbieder van een communicatiedienst zijn vastgelegd gedurende een periode van zes maanden voorafgaand aan de datum van de vordering;
b. ingeval van een redelijk vermoeden dat een misdrijf wordt beraamd of gepleegd waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld; de gegevens, bedoeld in artikel 13.2a, derde lid, onderdeel a, van de Telecommunicatiewet, die door de aanbieder van een communicatiedienst zijn vastgelegd gedurende een periode van twaalf maanden voorafgaand aan de datum van de vordering;
4. Een vordering als bedoeld in het derde lid kan slechts worden gedaan na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 126*l*, zevende lid, is van overeenkomstige toepassing.
5. Een vordering als bedoeld in het derde lid is schriftelijk en vermeldt:
a. indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon over wie gegevens worden gevorderd;
b. (een zo nauwkeurig mogelijke aanduiding van) de gegevens die worden gevorderd;
c. de periode waarover de vordering zich uitstrekt.

2. In het zevende lid (nieuw) wordt, onder vernummering van onderdeel e tot onderdeel f, een onderdeel e ingevoegd, luidende:

e. indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder *a*, de periode waarover de vordering zich uitstrekt;

C

Artikel 126zh, tweede lid, komt te luiden:

2. Artikel 126*n*, tweede tot en met negende lid, is van overeenkomstige toepassing.

Artikel III

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren wie zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven te – plaats -, - datum -

De Minister van Veiligheid en Justitie,

De Minister van Economische Zaken,

MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Dit wetsvoorstel voorziet in aanpassing van het Wetboek van Strafvordering en de Telecommunicatiewet vanwege het arrest van het Hof van Justitie van de Europese Unie (hierna: Hof van Justitie) in de gevoegde zaken Digital Rights Ireland en Seitlinger (C-293/12 en 294/12). In dit arrest heeft het Hof van Justitie de richtlijn 2006/24/EG[1] ongeldig verklaard. Dit wetsvoorstel voorziet in een bewaarplicht voor bepaald aangewezen telecommunicatiegegevens ten behoeve van de opsporing van ernstige misdrijven. Dit wetsvoorstel voorziet tevens in de nodige waarborgen ter bescherming en beveiliging van de bewaarde gegevens, die voortvloeien uit het arrest van het Hof van Justitie.

Mede namens de minister van Economische Zaken licht ik het wetsvoorstel in deze memorie van toelichting toe.

2. De hoofdlijnen van het wetsvoorstel

Dit wetsvoorstel voorziet in de aanpassing van de Telecommunicatiewet. Dit betreft vooraleerst de heroverweging van de termijnen voor het bewaren van bepaald aangewezen telecommunicatiegegevens ten behoeve van het algemene belang van de opsporing en vervolging van ernstige misdrijven, zodat deze worden vastgesteld op hetgeen strikt noodzakelijk is voor dat doel. Dit betreft zogenaamde historische verkeersgegevens; gegevens over het gebruik van telecommunicatie door personen. Daarbij worden de verschillende categorieën van te bewaren gegevens beperkt tot de gegevens die strikt noodzakelijk zijn voor de opsporing en vervolging van ernstige misdrijven. Voorts wordt voorgeschreven dat de telecommunicatiegegevens op het grondgebied van de Unie worden bewaard.
Dit wetsvoorstel voorziet tevens in de aanpassing van het Wetboek van Strafvordering. Dit betreft de beperking van de bevoegdheid van de officier van justitie tot het vorderen van historische verkeersgegevens. Voorgesteld wordt dat een dergelijke vordering slechts kan worden gedaan na voorafgaande rechterlijke toetsing. Tevens wordt de regeling van de toegang tot de bewaarde gegevens in verband met telefonie over een vast of mobiel netwerk en het internet (hierna ook: telefoniegegevens) aangepast, zodat de bewaarde gegevens slechts gedurende een periode van zes maanden kunnen worden

[1] Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (Pb L 105, blz. 54).

geraadpleegd ten behoeve van de opsporing of vervolging van strafbare feiten waarvoor voorlopige hechtenis mogelijk is. In vergelijking met de huidige bewaartermijn voor telefoniegegevens vormt dit een halvering van de periode gedurende welke de gegevens beschikbaar zijn voor de opsporing van dergelijke strafbare feiten. Voor de feiten waarvoor gevangenisstraf van ten minste acht jaar of meer kan worden opgelegd kunnen de bewaarde telefoniegegevens die gedurende de volledige bewaartermijn zijn vastgelegd, worden geraadpleegd. Dit betreft een termijn van twaalf maanden. Aldus wordt nadere differentiatie aangebracht in de beschikbaarstelling van de gegevens ten behoeve van de criminaliteitsbestrijding. Deze differentiatie is niet van toepassing op de beschikbaarstelling van gegevens in verband met internettoegang en bepaalde vormen van internettelefonie (hierna ook te noemen: internetgegevens), vanwege de kortere bewaartermijn voor deze gegevens, te weten zes maanden.

3. De noodzaak tot aanpassing van de wettelijke regeling voor de bewaring van telecommunicatiegegevens

In het arrest van 8 april 2014 heeft het Hof van Justitie – op verzoek van het Ierse High Court en het Oostenrijkse Verfassungsgerichtshof - de geldigheid van de Europese richtlijn onderzocht, in het bijzonder in het licht van twee door het Handvest van de grondrechten van de Europese Unie gewaarborgde grondrechten, te weten het recht op bescherming van het privéleven (artikel 7 van het Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 van het Handvest). Uit de toetsing van de verschillende bepalingen van de richtlijn dataretentie volgde volgens het Hof van Justitie dat de richtlijn dataretentie geen duidelijke en precieze regels stelde over de mate van aantasting van de fundamentele rechten van het Handvest van de grondrechten. Het Hof van Justitie oordeelde dat gelet op alle overwegingen de wetgever van de Unie met de vaststelling van de richtlijn dataretentie de door het evenredigheidsbeginsel gestelde grenzen had overschreden die hij in het licht van de artikelen 7, 8 en 52, eerste lid, van het Handvest van de grondrechten in acht had dienen te nemen.

De door het Hof van Justitie gewraakte bepalingen van de voormalige richtlijn dataretentie zijn destijds omgezet in de nationale wetgeving met de Wet bewaarplicht telecommunicatiegegevens. Toetsing van de Wet bewaarplicht telecommunicatiegegevens aan het Handvest leidt tot de conclusie dat deze wet moet worden aangepast. In een afzonderlijke beleidsreactie (Kamerstukken II 2014/15, P.M.) is het kabinet nader ingegaan op de diverse eisen die het Hof van Justitie heeft gesteld aan de opslag van (telecommunicatie)gegevens en daarbij aangeven op welke punten de Wet bewaarplicht telecommunicatiegegevens aanpassing behoeft. Met dit wetsvoorstel wordt uitvoering gegeven aan de in die reactie uitgewerkte voornemens.

Nu de richtlijn dataretentie ongeldig is verklaard, vormt de richtlijn 2002/58/EG[2] (hierna ook: e-privacyrichtlijn) het kader waarbinnen de omgang met telecommunicatiegegevens wordt geregeld. Op grond van deze richtlijn kunnen de lidstaten regels stellen voor het bewaren van telecommunicatiegegevens, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van bepaalde belangen, waaronder het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Daartoe kunnen lidstaten onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode voor die doelen te bewaren. Deze maatregelen dienen in overeenstemming te zijn met het gemeenschapsrecht, met inbegrip van de beginselen, bedoeld in het Handvest van de grondrechten en het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

4. De noodzaak van een bewaarplicht voor de opsporing en vervolging van ernstige misdrijven

De bewaarplicht houdt in dat bedrijven die telefonie en internet aanbieden, de verplichting hebben bepaalde verkeersgegevens te bewaren zodat deze beschikbaar blijven in het geval de gegevens noodzakelijk zijn in een opsporingsonderzoek naar een ernstig strafbaar feit. Dit betreft voor telefonie gegevens over onder meer het nummer van oproeper en opgeroepene bij het begin van de verbinding, tijd, duur van gesprek en locatie bij het begin van de verbinding. De inhoud van een gesprek of de inhoud van een sms-bericht valt niet onder de bewaarplicht. Historische verkeersgegevens van internet betreffen onder andere het e-mailadres van zender en ontvanger en de verkeersgegevens bij internettelefonie, anders dan internettelefonie via een vast of mobiel netwerk. De inhoud van gesprekken, berichten of e-mails, zoektermen die zijn ingetypt in een zoekmachine en IP-adressen van bezochte internetpagina's vallen niet onder de bewaarplicht. Indien er geen verplichting is voor deze aanbieders om de verkeersgegevens te bewaren voor de opsporing en vervolging van ernstige misdrijven, dan mogen de gegevens door de aanbieders uitsluitend worden bewaard ten behoeve van hun bedrijfsvoering. De situatie van nu is anders dan de situatie van vóór de invoering van de bewaarplicht (met uitzondering van de telecommunicatiegegevens voor prepaid gebruikers die gedurende drie maanden werden bewaard). In 2009 was het voor aanbieders noodzakelijk om voor bedrijfsdoeleinden verkeersgegevens en internetgebruikersgegevens 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 hebben dat veel verkeersgegevens en

[2] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Pb L 201 blz. 37).

internetgebruikersgegevens direct nadat de communicatie heeft plaatsgevonden vernietigd worden.

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 of 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 dagen, weken of 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 enige tijd na het moment van het plegen van het delict in beeld door middel van bijvoorbeeld getuigenverklaringen, forensisch onderzoek, het opvragen en onderzoeken van bewakingscamera's, na onderzoek van het netwerk van het slachtoffer of het nagaan van de bewegingen van het slachtoffer in de dagen vóór het misdrijf. Zonder de telefonie- en internetgegevens kan niet worden vastgesteld welke contacten het slachtoffer had of wie op of in de omgeving van de locatie van de plaats delict was als er geen getuigen zijn. Inzicht in de historische gegevens zorgt voor het uitsluiten of juist identificeren van mogelijke daders.

Ook in de jurisprudentie blijkt het belang van de historische verkeersgegevens. In een specifieke zaak heeft de rechtbank historische gegevens en zendmastgegevens, mede gelet op afgelegde verklaringen van de getuigen-deskundigen, voldoende betrouwbaar geacht om als bewijs te kunnen dienen. De rechtbank nam daarbij als uitgangspunt dat historische gegevens en zendmastgegevens in beginsel een ondersteunend karakter hebben maar dat die gegevens in onderling verband beschouwd en in samenhang met andere uit het dossier blijkende feiten en omstandigheden voor de bewezenverklaring redengevend kunnen zijn.

Het belang en de noodzaak van deze gegevens voor de opsporing blijkt niet alleen uit een veelheid aan casuïstiek, maar ook uit het onderzoek van het WODC in het kader van de evaluatie van de Wet bewaarplicht telecommunicatiegegevens. Het WODC stelde vast dat de historische gegevens over telefonie en internet veelvuldig worden opgevraagd en geanalyseerd om

sturing te kunnen geven aan het opsporingsonderzoek en verdachten te kunnen identificeren. Vooral voor het in kaart brengen van netwerken en het lokaliseren van een telefoon wordt veelvuldig een beroep gedaan op verkeers- en locatiegegevens. Daarnaast hebben de resultaten van het WODC onderzoek en de ervaringen uit de opsporingspraktijk laten zien dat het 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. Niettemin meent het kabinet dat het arrest van het Hof van Justitie tot een heroverweging van de bewaartermijnen en een beperking van de toegang tot bewaarde gegevens noodzaakt.

De regering is dan ook overtuigd van het belang en de onmisbaarheid van een bewaarplicht voor telecommunicatiegegevens voor de opsporing en vervolging van ernstige misdrijven en stelt daarom voor deze verplichting te handhaven.

5. De bewaartermijn

Het Hof van Justitie overwoog dat in de richtlijn dataretentie geen onderscheid werd gemaakt in de categorieën van gegevens en hun mogelijke betekenis voor het nagestreefde doel (punt 63). Verder was in de richtlijn niet bepaald dat de vaststelling van de bewaartermijn – die tussen de zes en vierentwintig maanden moet zijn - gebaseerd moest zijn op objectieve criteria, zodat gewaarborgd was dat deze was beperkt tot wat strikt noodzakelijk is (punt 64).

De bewaartermijnen van ten hoogste twaalf maanden voor telefoniegegevens en zes maanden voor internetgegevens zijn strikt noodzakelijk voor het doel, te weten de opsporing van ernstige strafbare feiten, en kunnen vanuit het oogpunt van privacybescherming niet onevenredig worden beschouwd.

Zoals in paragraaf 3 is weergegeven volgt heeft het Hof van Justitie geoordeeld dat uit de toetsing van de verschillende bepalingen van de richtlijn dataretentie volgde dat de richtlijn geen duidelijke en precieze regels stelde over de mate van aantasting van de fundamentele rechten van het Handvest van de grondrechten. Het Hof van Justitie heeft overwogen dat de richtlijn bepaalde dat de bewaartermijn varieerde van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat werd gepreciseerd dat deze termijn op basis van objectieve criteria moest worden vastgesteld om te waarborgen dat deze beperkt is tot wat strikt noodzakelijk is. Gegeven de privacy en terughoudendheid die daarbij hoort als reactie op de uitspraak van het Hof van Justitie lijkt harmonisering van de bewaartermijn, in die zin dat voor zowel telefoniegegevens als internetgegevens een bewaartermijn van twaalf maanden geldt, niet opportuun. Bij het bepalen van de bewaartermijn dienen zowel de privacyaspecten als de noodzakelijkheid voor de opsporing te worden betrokken. Met inachtneming daarvan wordt voorgesteld de bewaartermijnen onveranderd te laten. Dat wil zeggen, een bewaartermijn van zes maanden voor

internetgegevens en twaalf maanden voor telefoniegegevens. Om de aantasting van de persoonlijke levenssfeer in verband met de bewaring van telecommunicatiegegevens zoveel mogelijk te beperken wordt voorgesteld differentiatie aan te brengen in de toegang tot de bewaarde telefoniegegevens. Hierop wordt hieronder, in paragraaf 7, nader ingegaan.

Onderstaand is een selectie opgenomen van de vele voorbeelden uit de opsporingspraktijk om het grote belang van deze gegevens voor opsporing en vervolging te illustreren en nader te onderbouwen waarom de gegevens voor een bepaalde periode beschikbaar moeten blijven.

In de zaak Robert M. zijn de historische verkeersgegevens van cruciaal belang geweest om bewijs te verzamelen voor het grootschalig misbruik, maar ook om slachtoffers en medeverdachten in beeld te krijgen. In 2011 bedroeg de bewaartermijn voor internetgegevens overigens nog twaalf maanden. Indien de bewaartermijn destijds zes maanden was geweest, zoals thans het geval, had dit grote consequenties gehad voor het identificeren van de slachtoffers en medeverdachten. In deze zaak zijn naar aanleiding van de analyse van de chatgesprekken zogenaamde quick scans opgesteld, waarin werd beschreven welke contacten een (op dat moment al dan niet geïdentificeerde) persoon met de vermoedelijke hoofdverdachte had onderhouden. Van deze quick scans zijn vervolgens zesenzeventig scans aan meerdere politieregio's overgedragen met het verzoek om nader onderzoek te doen. In bijna alle gevallen kon een in de chat gebruikte gebruikersnaam worden gekoppeld aan een IP-adres, dat kon worden herleid tot een Nederlandse internet serviceprovider. Door middel van het vorderen van gebruikersgegevens bij die aanbieders konden veel Nederlandse verdachten worden geïdentificeerd. Naar aanleiding van dit opsporingsonderzoek zijn ook in het buitenland opsporingsonderzoeken verricht en zijn tot op heden meer dan honderdvijftig verdachten aangehouden en meer dan honderd kinderen uit een actuele misbruiksituatie bevrijd. Met uitzondering van een (zeer) beperkt aantal gevallen was een gebruikt IP-adres de enige aanwijzing die kon leiden tot de identiteit van een verdachte of een slachtoffer.

Een internationaal onderzoek naar kindermisbruik was minder succesvol. Het betrof een website waarop kinderporno werd getoond, waar hyperlinks naar andere websites stonden en waar gebruikers kinderporno konden up- of downloaden of van commentaar konden voorzien. In het internationale onderzoek was het gelukt om zeer veel IP-adressen van gebruikers van deze omgeving te achterhalen. Daaronder vielen meer dan honderd Nederlanders. Geen van deze zaken kon in behandeling genomen worden, omdat de bewaartermijn was verlopen en dus de enige aanknopingspunten, te weten de IP-adressen, niet meer bruikbaar waren. Andere onderzoeksmogelijkheden ontbraken.

Indien de telefonie- en internetgegevens niet meer beschikbaar zijn, kunnen verdachten in zaken als bovengenoemd niet meer opgespoord en vervolgd worden. Dit heeft niet alleen tot gevolg dat mogelijke bezitters van kinderpornografisch materiaal niet opgespoord worden, maar ook dat zogenaamde "groomers" niet opgespoord worden en door kunnen gaan met hun handelingen. Ook eventueel achterliggend kindermisbruik kan daardoor niet gesignaleerd worden, waardoor misbruiksituaties rond zeer jonge slachtoffers zullen kunnen voortduren.

Om een verdachte in relatie te kunnen brengen met een gepleegd delict kan het noodzakelijk zijn een beeld te vormen van zijn of haar gedragspatroon. Om dergelijke patronen te kunnen vaststellen is het noodzakelijk om, in het bijzonder telefoniegegevens, over een langere periode op te vragen en dus te bewaren. Over een korte periode kan geen gedragspatroon worden vastgesteld en wordt het ook moeilijk om afwijkingen in het gedragspatroon te benoemen. Wanneer dit patroon inzichtelijk is kan worden beoordeeld of er afwijkingen zijn te benoemen die een direct verband tonen met het delict. Daarnaast kunnen, als de termijn lang genoeg is, vaste contacten worden geïdentificeerd. Dit kan van cruciaal belang zijn als een verdachte van een groep is geïdentificeerd terwijl nog wordt gezocht naar de overige leden. De gegevens kunnen ook voor het uitsluiten van verdachten van doorslaggevend belang zijn. Verklaringen van verdachten kunnen worden geverifieerd of weerlegd met behulp van historische verkeersgegevens. Het belgedrag of de locatie van de telefoon op het moment van het plegen van het delict kan het alibi van een verdachte bevestigen of ontkrachten. In een drievoudige moordzaak waarin de verklaringen van verdachten onderling sterk van elkaar afweken, is er slechts gebruik gemaakt van verklaringen als deze in belangrijke mate werden ondersteund door andere (objectieve) gegevens. De telecomanalyse heeft hierbij een cruciale rol gespeeld daar deze analyse meermalen ondersteuning of weerlegging opleverde van afgelegde verklaringen.

Ook voor de bestrijding van mensenhandel is een bewaartermijn van twaalf maanden voor telefoniegegevens van groot belang. Slachtoffers van mensenhandel komen niet zelden pas na geruime tijd tot een aangifte of tot het afleggen van een verklaring bij de politie. De redenen hiervoor zijn divers: angst voor de uitbuiters, financiële afhankelijkheid van de uitbuiters, zich niet vrij kunnen bewegen, psychische traumaverwerking of in een nieuwe uitbuitingssituatie betrokken zijn geraakt. Ook voor de gevallen dat een slachtoffer pas na maanden besluit om naar de politie te gaan of aangifte te doen, is het noodzakelijk dat de historische gegevens over een voldoende lange termijn beschikbaar zijn. Als een slachtoffer zich uit haar misbruiksituatie weet te bevrijden kan door het opvragen van de historische verkeersgegevens van het slachtoffer over een langere periode, een koppeling worden gemaakt met een verdachte. Zo ook in een zaak van twintigjarig slachtoffer die via hulpverlening aan haar misbruiksituatie wist te ontsnappen. Door het opvragen en analyseren

van de historische verkeersgegevens van het slachtoffer over een periode van twaalf maanden was de politie in staat om telefoonnummers te koppelen aan een verdachte. Dankzij de verkeersgegevens werden reisbewegingen van telefoontoestellen vastgesteld. Uit de analyse bleek dat het telefoontoestel van de verdachte en het telefoontoestel van het slachtoffer zich gelijktijdig naar diverse plaatsen in Nederland verplaatsten en in de nabijheid van het prostitutiegebied, dan wel seksclubs verbleven. Vastgesteld kon worden dat de telefoon van het slachtoffer op die locaties bleef terwijl die van de verdachte dagelijks heen en weer reisde naar zijn woonplaats. Dit patroon kwam overeen met de verklaring van het slachtoffer. Uit de verkeersgegevens van de telefoons van de verdachte en het slachtoffer bleek dat zij, gedurende langere periode, gemiddeld meer dan vijftig keer per dag telefonisch contact met elkaar hadden. Dit is een fenomeen dat bij mensenhandel vaak voorkomt en dat de mate van controle die de verdachte op het slachtoffer uitoefent bevestigt. Het behoeft geen toelichting dat de verdachte ontkent en dat dergelijke zaken veelal in het bijzonder dankzij de historische verkeersgegevens kunnen leiden tot een veroordeling.

Op basis van deze voorbeelden, en nog vele andere voorbeelden die beschikbaar zijn, kan worden geconcludeerd dat er meerdere redenen zijn waarom het langer beschikbaar hebben van de telecommunicatiegegevens noodzakelijk is. Op de plaats van het delict worden allerlei fysieke sporen vastgelegd die richting kunnen geven naar een potentiele dader. De analyse van deze gegevens, zoals DNA, neemt enige tijd in beslag. Wanneer op basis van deze analyses een verdachte kan worden geïdentificeerd, kunnen telecommunicatiegegevens van deze verdachte worden opgevraagd.
Daarnaast komt het (in het bijzonder) bij zedendelicten regelmatig voor dat slachtoffers van kinderporno zich om meerdere redenen (onder andere angst en/of late ontdekking van het strafbare feit) pas later melden bij de politie. Dit kan tot gevolg hebben dat er geen gebruikers- en verkeersgegevens meer beschikbaar zijn, waardoor zaken niet (verder) opgepakt kunnen worden. Ten slotte is het bij internationale rechtshulpverzoeken niet ongebruikelijk dat een land pas geruime tijd na aanvang van het eigen onderzoek een verzoek om rechtshulp richt aan de Nederlandse autoriteiten. Dit is in het bijzonder het geval in terreurzaken, bij zware (georganiseerde) criminaliteit en bij onderzoeken die zich richten op het ontnemen van wederrechtelijk verkregen voordeel.

In dit verband wijs ik ook op de recent aan u toegezonden Veiligheidsagenda (Kamerstukken ...). In deze agenda zijn door de veiligheidspartners doelstellingen en prestaties geformuleerd rondom een aantal fenomenen, zoals cybercriminaliteit en de aanpak van (het aanzetten tot) jihadisme/terrorisme. Bij de laatste algemene beschouwingen zijn de aanpak van cybercrime en internationale samenwerking, ook op het gebied van kinderporno en misbruik van kinderen als prioriteit bestempeld. Het behoeft nauwelijks betoog dat het slagen in deze ambities mede wordt bepaald door de slagkracht van de

opsporing. Deze is gebaat bij mogelijkheden om telecommunicatiegegevens gedurende langere tijd te bewaren en te gebruiken.

Voor wat betreft het onderscheid tussen de verschillende categorieën van gegevens naar gelang het nut ervan voor het nagestreefde doel, kan worden opgemerkt dat de bewaartermijnen van twaalf en zes maanden gelden voor de gegevens van alle personen, ongeacht de mate van hun betrokkenheid bij ernstige misdrijven. Indien de gegevens zijn gevorderd ten behoeve van het opsporingsonderzoek naar ernstige misdrijven en relevant blijken voor de opsporing of vervolging van ernstige misdrijven, dan gelden andere termijnen voor de verdere verwerking van de gegevens door de politie of het openbaar ministerie. Deze termijnen zijn vastgelegd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Als de gegevens op grond van de vordering van de officier van justitie door de aanbieder van de telecommunicatiedienst worden verstrekt ten behoeve van een opsporingsonderzoek, dan is het regime van de Wet politiegegevens van toepassing op de verdere verwerking van de gegevens. De gegevens kunnen worden verwerkt zolang als nodig voor het doel van het onderzoek (artikel 9, vierde lid, Wpg).

6. De te bewaren gegevens

Met de Wet bewaarplicht telecommunicatiegegevens is een lijst van gegevens vastgesteld die dienen te worden bewaard ten behoeve van de opsporing en vervolging van strafbare feiten. In deze lijst van de te bewaren gegevens, die als bijlage bij artikel 13.2a van de Telecommunicatiewet is vastgesteld, wordt onderscheid gemaakt tussen (internet)telefonie door middel van een vast of mobiel netwerk enerzijds en internettoegang en overige vormen van internettelefonie anderzijds. Bij bepaalde vormen van internettelefonie, zoals Voice over IP (VoIP), komen de functionaliteit en de gegenereerde verkeersgegevens overeen met die van een openbare telefoondienst, als bedoeld in de Telecommunicatiewet (artikel 1.1, onder x. Tw). Voor de verkeersgegevens van deze vormen van telefonie geldt dan een bewaartermijn van twaalf maanden. Hiermee wordt aangesloten bij de bestaande regeling (Kamerstukken II, 2009/10, 32 185, nrs. 3 en 6).

Naar aanleiding van het arrest van het Hof van Justitie 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 over te gaan tot schrapping van de gegevens met betrekking tot e-mail over internet. Tevens wordt voorgesteld om niet langer de datum en tijdstip van de log-in en log-off van een internetsessie gebaseerd op een bepaalde tijdzone samen met het IP-adres op te slaan. Tenslotte is de verplichting tot bewaring van

locatiegegevens, anders dan de locatieaanduiding bij het begin van de verbinding (de zogenaamde first Cell ID), overbodig. Dit betreft de locatiegegevens die zijn aangewezen in het Besluit bijzondere vergaring nummers telecommunicatie, op basis van artikel 13.4, derde lid, van de Telecommunicatiewet. Voorgesteld wordt deze verplichting te schrappen omdat de politie inmiddels over andere methoden beschikt om de betreffende gegevens te achterhalen.

De bedoeling van de bewaarplicht voor telecommunicatiegegevens is dat gegevens beschikbaar zijn voor opsporing en vervolging zodat de abonnee of gebruiker van telecommunicatie kan worden geïdentificeerd. In de praktijk blijken er echter verschillende interpretaties van de term IP-adres als bedoeld in de bijlage, behorende bij artikel 13.2a van de Telecommunicatiewet, mogelijk. Voorgesteld wordt om de formulering aan te passen zodat IP-adressen voortaan te relateren zijn aan een individuele gebruiker of abonnee.

7. De toegang tot de bewaarde gegevens

Het Hof van Justitie overwoog dat de richtlijn geen objectief criterium bevatte ter beperking van het aantal personen dat werd geautoriseerd voor de toegang en het verdere gebruik van de gegevens, tot hetgeen strikt noodzakelijk was in het licht van de te bereiken doelen. Bovenal was de toegang van de bevoegde autoriteiten tot de bewaarde gegevens niet afhankelijk gesteld van voorafgaande toetsing door een gerecht of een onafhankelijk bestuurlijk orgaan naar aanleiding van een gemotiveerd verzoek van de aangewezen autoriteiten (punt 62).

Met inachtneming van de regeling van de eerdergenoemde e-privacyrichtlijn worden de telecommunicatiegegevens uitsluitend bewaard ten behoeve van bepaalde doeleinden van het algemeen belang. Dit betreft de opsporing en vervolging van ernstige misdrijven. Dit zijn misdrijven waarvoor voorlopige hechtenis mogelijk is. Deze misdrijven zijn opgesomd in artikel 67, eerste lid, van het Wetboek van Strafvordering.

Aan het vereiste van de vaststelling van de bewaartermijn op basis van objectieve criteria, zodat gewaarborgd is dat deze is beperkt tot wat strikt noodzakelijk is, wordt nader vorm gegeven doordat de toegang tot de gegevens met betrekking tot telefonie over een vast of mobiel netwerk ten behoeve van de opsporing van ernstige misdrijven wordt beperkt aan de hand van de ernst van het betreffende misdrijf. Naast de termijn die geldt voor het bewaren van gegevens door de telecombedrijven is de termijn voor de daadwerkelijke toegang tot de gegevens door de officier van justitie van doorslaggevend belang voor het vaststellen van de noodzakelijkheid en de proportionaliteit van dit systeem van gegevensverwerking. Het stellen van voorwaarden aan de toegang betreft een nieuwe, aanvullende maatregel ter bevordering van een zorgvuldige omgang met de bewaarde telefoniegegevens.

De nadere regeling van de toegang komt op het volgende neer. De bewaartermijn is voor de gegevens met betrekking tot telefonie over een vast of mobiel netwerk en via het internet vastgesteld op twaalf maanden. De gegevens worden bewaard door de aanbieders en bevinden zich feitelijk nog niet bij het openbaar ministerie of politie. Om toegang tot de gegevens te verkrijgen is een vordering van de officier van justitie vereist. De bewaartermijn van twaalf maanden kan, anders dan tot nu toe, door de officier van justitie echter alleen volledig worden benut wanneer sprake is van de zwaarste categorie delicten, met een strafbedreiging van acht jaar of meer. Bij lichtere delicten, waarvoor voorlopige hechtenis kan worden opgelegd maar waarop geen strafbedreiging van acht jaar of meer is gesteld, 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 aanbieders, maar kan de officier van justitie de gegevens niet meer vorderen. Dit betekent in feite dat de periode van beschikbaarheid van de bewaarde gegevens voor de opsporing van ernstige misdrijven, waarvoor voorlopige hechtenis kan worden opgelegd maar waarop geen gevangenisstraf van acht jaar of meer is gesteld, wordt teruggebracht van twaalf naar zes maanden.

Hierbij wordt dus onderscheid gemaakt tussen misdrijven waarvoor voorlopige hechtenis mogelijk is en misdrijven waarvoor eveneens voorlopige hechtenis mogelijk is maar waarop een gevangenisstraf van acht jaar of meer is gesteld. Voor de eerstgenoemde categorie van ernstige misdrijven kan worden gedacht aan misdrijven als deelneming aan een criminele organisatie (art. 140 Sr), diefstal (art. 310 Sr), oplichting (art. 326 Sr). Voor de laatstgenoemde categorie van zeer ernstige misdrijven kan worden gedacht aan delicten als mensenhandel (art. 273f, eerste lid, Sr) of ernstige vormen van kinderpornografie (art. 240b, tweede lid, Sr). Voor de strafbare feiten waarvoor voorlopige hechtenis mogelijk is kunnen de bewaarde gegevens slechts worden geraadpleegd gedurende een termijn van zes maanden voorafgaand aan de datum van de vordering. Dit betreft een halvering van de periode van beschikbaarheid van de gegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven, omdat dergelijke gegevens thans twaalf maanden beschikbaar zijn. Voor de feiten waarvoor gevangenisstraf van ten minste acht jaar of meer kan worden opgelegd kunnen de bewaarde gegevens over een langere periode worden geraadpleegd, namelijk gedurende een periode van twaalf maanden voorafgaand aan de datum van de vordering. Aldus kan aan de hand van een objectief criterium, te weten de ernst van het betreffende strafbare feit, nadere differentiatie worden aangebracht in de beschikbaarstelling van de gegevens ten behoeve van de criminaliteitsbestrijding.

Voor de gegevens in verband met internettoegang en bepaalde vormen van internettelefonie is de bewaartermijn vastgesteld op zes maanden, vanaf de datum van de communicatie. De bewaarde gegevens kunnen gedurende deze

periode worden geraadpleegd ten behoeve van de opsporing van strafbare feiten waarvoor voorlopige hechtenis mogelijk is.

De telecommunicatiegegevens worden door de aanbieders bewaard ten behoeve van de strafrechtelijke handhaving van de rechtsorde, meer in het bijzonder de opsporing en vervolging van ernstige misdrijven. Naar aanleiding van het arrest van het Hof van Justitie wordt voorgesteld de toegang tot de bewaarde verkeersgegevens afhankelijk te stellen van een voorafgaande rechterlijke toetsing, zodat kan worden verzekerd 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. Dit past goed in het wettelijke systeem van de inzet van bijzondere opsporingsbevoegdheden.

De opsporingsambtenaar is bevoegd, ingeval van een verdenking van een misdrijf of ingeval van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, in het belang van het onderzoek historische gebruikersgegevens te vorderen (artikel 126na/ua Sv). Een soortgelijke bevoegdheid geldt ingeval van aanwijzingen van een terroristisch misdrijf (artikel 126zi Sv). Het betreft hier gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst. Uit deze gegevens kunnen geen precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals dat naar het oordeel van het Hof van Justitie aan de orde is bij de bewaring van de verkeersgegevens op grond van de richtlijn dataretentie (punt 27). De huidige wettelijke regeling voor het vorderen van deze gegevens, die niet voorziet in een voorafgaande machtiging van de rechter-commissaris, behoeft op dit punt dan ook geen aanpassing.

8. Gegevensbescherming en gegevens beveiliging (de bescherming en beveiliging van de bewaarde gegevens)

Het Hof van Justitie overwoog dat de richtlijn niet voorschreef dat de betrokken gegevens op het grondgebied van de Unie werden bewaard, zodat niet ten volle was gewaarborgd dat een onafhankelijke autoriteit toezicht hield op de inachtneming van de vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk voorgeschreven door artikel 8, derde lid, van het Handvest van de grondrechten (punt 68).

Naar aanleiding hiervan wordt voorgesteld de Telecommunicatiewet aan te passen, zodat voorgeschreven wordt dat de te bewaren gegevens worden opgeslagen en verwerkt in Nederland of in een andere lidstaat van de Europese Unie. Doordat de gegevens worden bewaard op het grondgebied van de Unie is

beter gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk voorgeschreven in het Handvest van de grondrechten (artikel 8, derde lid, Handvest).

Het Besluit beveiliging gegevens telecommunicatie (Bbgt) bepaalt dat beveiligingsmaatregelen moeten worden genomen. Zo moeten de gegevens die de aanbieders sinds 2009 moeten bewaren, worden opgeslagen in een database die in een beveiligde omgeving staat. Deze gegevens mogen slechts voor een beperkt aantal medewerkers van de aanbieder toegankelijk zijn. Alleen medewerkers die werkzaam bij de betreffende aanbieder en die vanuit hun functie in aanraking komen met het behandelen van vorderingen van behoeftestellers hebben toegang tot deze gegevens. Deze gegevens worden opgeslagen met als doel de opsporing en vervolging van ernstige strafbare feiten, en zijn te onderscheiden van de gegevens die door de aanbieders worden bewaard ten behoeve van de eigen bedrijfsvoering. Het ligt dan ook in de rede om de gegevens die ten behoeve van de opsporing en vervolging worden bewaard, beter af te schermen tegen feitelijke inzage door onbevoegden. De regering zal onderzoeken of de aangescherpte beveiliging door middel van versleuteling van de bewaarde gegevens kan plaatsvinden. Op grond van de Telecommunicatiewet kunnen nadere regels worden gesteld over de te nemen maatregelen in verband met de beveiliging van de bewaarde gegevens en de waarborging dat de toegang tot de gegevens slechts mogelijk is voor speciaal daartoe bevoegde personen (artikel 13.5, vierde lid, Tw). Aldus kunnen in het Bbgt nadere regels worden opgenomen over de versleuteling van de bewaarde gegevens.

9. Bedrijfseffecten

Het wetsvoorstel zal gevolgen kunnen hebben voor de administratieve lasten van het openbaar ministerie en de zittende magistratuur. Dit houdt vooraleerst verband met de voorgestelde rechterlijke toetsing, voorafgaand aan de toegang tot de bewaarde gegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven. Het vereiste van de machtiging van de rechter-commissaris zal leiden tot verhoging van de administratieve lasten aan de zijde van het openbaar ministerie en de rechtspraak. In samenwerking met de politie, het openbaar ministerie en de zittende magistratuur zal een impact analyse worden uitgevoerd naar de effecten van het wetsvoorstel op de bedrijfsvoering van deze instanties.

Het wetsvoorstel zal tevens gevolgen kunnen hebben voor de bedrijfsvoering van de in Nederland opererende internet- en telecomaanbieders. De verplichting tot opslag van de gegevens op het grondgebied van de Europese Unie kan consequenties hebben voor de bedrijfsvoering en de kosten van de aanbieders. De precieze bedrijfseffecten en kosten zullen in samenwerking met het bedrijfsleven nader in kaart worden gebracht.

10. De adviezen over het wetsvoorstel

P.M.

ARTIKELSGEWIJS DEEL

Artikel I

Wijziging van de Telecommunicatiewet

Onderdeel A

Artikel 13.2a

Tweede lid
De aanbieders bewaren de in de bij deze wet behorende bijlage aangewezen gegevens, voor zover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, gedurende een periode van zes of twaalf maanden, gerekend vanaf de datum van de communicatie, teneinde te kunnen voldoen aan een vordering op grond van artikel 126n, artikel 126u of artikel 126zh van het Wetboek van Strafvordering. Dit lid betreft de verplichting voor de aanbieders om de gegevens die zijn opgenomen in de bij deze wet behorende bijlage te bewaren. De gegevens worden voor de aanbieders bewaard met het oog op het algemene belang van de opsporing en vervolging van ernstige strafbare feiten, teneinde te kunnen voldoen aan een vordering van de officier van justitie tot verstrekking van historische verkeersgegevens. Een dergelijke vordering is uitsluitend mogelijk bij verdenking van een ernstig misdrijf, waarvoor voorlopige hechtenis mogelijk is. Met de voorgestelde wijziging wordt het doel van de bewaring preciezer omschreven en een objectief criterium geboden ter begrenzing van de toegang van de bevoegde autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen. Hiermee wordt tegemoet gekomen aan het arrest van het Hof van Justitie (punt 60).

Onderdeel B

Artikel 13.4

Eerste lid
Dit betreft het herstel van een omissie. Met de Wet bewaarplicht telecommunicatiegegevens is dit artikel gewijzigd, waarbij de vorderingsbevoegdheden op grond van het Wetboek van Strafvordering en de

Wet op de inlichtingen- en veiligheidsdiensten in één bepaling zijn samengebracht. De verplichting voor de aanbieders op basis van dit lid betreft de vordering of het verzoek tot verstrekking van verkeersgegevens. Deze vordering betreft een vordering op grond van artikel 126n of 126u Sv. De verplichting voor de aanbieders op grond van het tweede lid betreft de vordering of het verzoek tot verstrekking van gebruikersgegevens. Deze vordering betreft een vordering op grond van artikel 126na of 126ua Sv. Thans wordt in het eerste lid echter ook verwezen naar de vordering tot verstrekking van gebruikersgegevens. Dat is niet alleen verwarrend maar bovendien overbodig omdat de vordering tot verstrekking van verkeersgegevens ook de gebruikersgegevens omvat. Daarom wordt voorgesteld in dit lid de verwijzingen naar de vordering van gebruikersgegevens te schrappen. Dit impliceert schrapping van de verwijzing naar de artikelen 126na en 126ua Sv.

Tevens wordt voorgesteld een verwijzing naar artikel 126zh Sv in te voegen. Dit betreft de bevoegdheid van de officier van justitie tot het vorderen van verkeersgegevens, ingeval van aanwijzingen van een terroristisch misdrijf. Ten onrechte is in dit lid niet de verplichting van de aanbieders opgenomen om aan een degelijke vordering te voldoen. Met de voorgestelde wijziging wordt deze omissie hersteld.

Derde lid
Dit betreft een technische wijziging. In artikel 13.4, derde lid, van de Telecommunicatiewet is een beperkte bewaarplicht opgenomen ten behoeve van de zogenaamde bestandsanalyse. Deze analyse houdt in dat als de aanbieder niet kan voldoen aan zijn verplichting om op vordering van een bevoegde autoriteit gegevens over een gebruiker van telecommunicatie te verstrekken, hij deze gegevens door middel van een analyse van zijn bestanden achterhaalt. Dit doet zich voor als de gegevens over een gebruiker van telecommunicatie niet bij de aanbieder zijn geregistreerd, zoals bij prepaid mobiele telefonie. De bestandsanalyse is, als alternatief voor een registratieplicht van prepaid cardhouders, nodig om gebruikers van vooruitbetaalde diensten te kunnen identificeren in het belang van het opsporingsonderzoek naar strafbare feiten. Deze bestandsanalyse is uitgewerkt in het Besluit bijzondere vergaring nummergegevens[3]. Met de Wet bewaarplicht telecommunicatiegegevens is de bewaartermijn voor de in het Besluit bijzondere vergaring nummergegevens aangewezen gegevens verhoogd van drie naar twaalf maanden.

Voor zowel de bewaarplicht als de bestandsanalyse moeten de aanbieders dezelfde gegevens bewaren. Schrapping van de tweede volzin van dit lid levert meer duidelijkheid over de verplichtingen van de aanbieder. Dit betreft specifiek de beperking tot de zogenaamde first cell ID, en niet ook de last cell ID.

[3] Stb. 2002, 31.

Onderdeel C

Artikel 13.5, onderdeel c
Er zijn verschillende wetten en verschillende regels op het gebied van de gegevensbescherming en gegevensbeveiliging van toepassing op de gegevensverwerking door de aanbieders. Dit betreft in de eerste plaats de Wet bescherming persoonsgegevens (Wbp). De Wbp is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Ook de gegevensverwerking door de aanbieders in het kader van het aanbieden van openbare telecommunicatienetwerken en openbare telecommunicatiediensten valt onder de reikwijdte van deze wet. De Wbp bevat bepalingen omtrent de voorwaarden voor gegevensverwerking, doelbinding en de verdere verwerking van gegevens, de bewaartermijnen, de rechten van de betrokkene, rechtsbescherming en het toezicht. De verantwoordelijke dient de nodige maatregelen te treffen opdat de persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens verder verwerkt, juist en nauwkeurig zijn (artikel 11, tweede lid, Wbp). Ook is de verantwoordelijke verplicht passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of enige andere vorm van onrechtmatige gegevensverwerking (artikel 13 Wbp).

In aanvulling op de regels van de Wet bescherming persoonsgegevens zijn in de Telecommunicatiewet specifieke regels gesteld voor de verwerking van persoonsgegevens door de aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten. Dit houdt verband met de implementatie van de eerdergenoemde e-privacyrichtlijn. In deze richtlijn worden de beginselen van Richtlijn nr. 95/46/EG (privacyrichtlijn) omgezet in specifieke voorschriften voor de verwerking van persoonsgegevens in de sector elektronische communicatie van de Europese Unie. Anders dan de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de verwerking van gegevens betreffende natuurlijke personen, strekt de reikwijdte van de bepalingen van de e-privacyrichtlijn zich in beginsel ook uit tot rechtspersonen. De e-privacyrichtlijn is grotendeels geïmplementeerd in hoofdstuk 11 van de Telecommunicatiewet en de daarop berustende uitvoeringsregelgeving. Deze regels hebben onder meer betrekking op de doeleinden met het oog waarop de aanbieders verkeersgegevens kunnen verwerken, de duur van de gegevensverwerking, de veiligheid en de verstrekking van informatie over de gegevensverwerking aan de abonnee of gebruiker. De aanbieders zijn verplicht passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de aangeboden netwerken en diensten (artikel 11.3 Tw).

In aanvulling op de regels van de Wbp en de Telecommunicatiewet worden in het eerdergenoemde Bbgt nadere regels gesteld terzake van de bescherming en beveiliging van de te bewaren gegevens. Deze regels betreffen de technische en organisatorische maatregelen die de aanbieder moet treffen om de gegevens te beveiligen tegen vernietiging, verlies of wijziging en niet toegelaten opslag, verwerking, toegang of openbaarmaking en om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen.

Met een verplichting voor de aanbieders de te bewaren gegevens binnen de Europese Unie op te slaan en te verwerken kan beter worden gewaarborgd dat de opslag en verwerking voldoet aan de Europese normen op het gebied van de bescherming en beveiliging van de bewaarde gegevens. Deze normen houden verband met de implementatie van de privacyrichtlijn en de e-privacyrichtlijn door de lidstaten. Doordat de regels voor de bescherming en de beveiliging van de gegevens op Europees niveau redelijk gelijkvormig zijn, wordt met deze verplichting een minimumniveau voor de gegevensbescherming en -beveiliging gewaarborgd. Dit is een stap vooruit ten opzichte van de huidige situatie, op grond waarvan de te bewaren gegevens in derde landen kunnen worden opgeslagen, waar de Europese normen niet van toepassing zijn. Tevens wordt het toezicht op de naleving van die normen versterkt, omdat de lidstaten op grond van de eerdergenoemde Europese normen gehouden zijn een onafhankelijk toezichthoudend orgaan te belasten met het toezicht op de verwerking van persoonsgegevens.

Onderdeel D

Artikel 13.9
Dit betreft de aanpassing van de evaluatiebepaling. Nu het Hof van Justitie de richtlijn dataretentie met terugwerkende kracht ongeldig heeft verklaard ligt aanpassing van deze bepaling in de rede omdat daarin wordt verwezen naar de richtlijn dataretentie. Daar komt bij dat dit wetsvoorstel niet alleen voorziet in wijziging van de bepalingen in de Telecommunicatiewet die betrekking hebben op de bewaarplicht voor telecommunicatiegegevens, maar ook in de bepalingen van het Wetboek van Strafvordering die betrekking hebben op het vorderen van die gegevens ten behoeve van de opsporing van ernstige misdrijven. Voor de formulering van deze bepaling is aangesloten bij de aanwijzingen voor de regelgeving (aanwijzing 164).

Onderdeel E

Artikel 18.7
De door Onze Minister aangewezen ambtenaren zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Telecommunicatiewet met betrekking tot bevoegd aftappen en het bewaren van gegevens, als bedoeld in hoofdstuk 13 van de Telecommunicatiewet (art. 15, eerste lid, Tw). Daartoe is de

Minister van Economische Zaken bevoegd alle informatie te vorderen voor zover dat nodig is voor de vervulling van hun taak (art. 18.7 Tw). De verkeers- en locatiegegevens die door de aanbieders worden bewaard op grond van artikel 13.2a van die wet, zijn hiervan echter uitgezonderd, voor zover deze gegevens niet ten dienste van de eigen bedrijfsvoering worden verwerkt (Kamerstukken II, 2006/07, 31 145, nr. 3, blz. 55).

Aldus bestaat het toezicht op de beveiliging en vernietiging van gegevens die nodig zijn voor de opsporing op dit moment uit systeemtoezicht. Dat wil zeggen dat de toezichthouder aan de hand van een beschrijving die de aanbieder geeft van zijn bedrijfsvoeringsprocessen, beoordeelt 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. Daarvoor is noodzakelijk dat de toezichthouders bevoegd zijn om deze gegevens daadwerkelijk in te kunnen zien als bewijs voor de mate waarin de aanbieder gegevens verwijdert en als bewijs voor het beveiligingsniveau. In het eerdergenoemde onderzoek naar de evaluatie van de Wet bewaarplicht telecommunicatiegegevens door het WODC wordt daarover het volgende gemeld:

'Het AT heeft enkel de mogelijkheid om toe te zien op de juiste uitvoering van bedrijfsprocessen en beschikt niet over de instrumenten die nodig zijn om op de inhoud van de bewaarde en geleverde gegevens toe te kunnen zien. Het AT heeft niet de bevoegdheid om de daadwerkelijke output van verkeers- en locatiegegevens van verschillende aanbieders in te zien. Hiermee mist het Agentschap een instrument om dit aspect van het toezicht goed uit te kunnen voeren. Wanneer een overheid besluit privacygevoelige informatie van burgers op te slaan en te bewaren, hoort daar een solide en effectief toezicht bij. Het verdient daarom aanbeveling om de rol van de toezichthouder op dit vlak te verbeteren.'

Gelet hierop wordt voorgesteld dit artikel te wijzigen om de toezichthouders 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 diegene is er bij gebaat dat de toezichthouder feitelijk kan onderzoeken of de verwerking, beveiliging en vernietiging van gegevens plaats heeft conform de wettelijke voorschriften.

Door de minister van Economische Zaken aangewezen toezichthouders van het Agentschap Telecom zien, op grond van artikel 15.1, eerste lid, onderdeel i, van de Telecommunicatiewet, toe op de beveiliging en verwijdering van de gegevens die op grond van artikel 13.2a van de Telecommunicatiewet door de aanbieders worden bewaard. In het Besluit aanwijzing toezichthouders Telecommunicatiewet zijn de ambtenaren met de functienamen inspecteur, senior

inspecteur/medewerker toezicht van de afdeling Toezicht van Agentschap Telecom belast met het toezicht. Dit betekent dat de vordering op basis van 18.7, tweede lid, van de Telecommunicatiewet uitsluitend kan worden verricht door deze toezichthoudende ambtenaren. Andere toezichthouders (die aldus geen toezicht houden op de zogenoemde bewaarplicht) hebben geen toegang tot deze gegevens. Hiertoe strekt de clausulering "voor zover dit nodig is voor het toezicht op de naleving van het bepaalde bij of krachtens hoofdstuk 13".

Onderdeel F

Dit betreft de aanpassing van de lijst van de te bewaren gegevens. Voorgesteld wordt om de volgende gegevens te schrappen uit de bijlage behorende bij artikel 13.2a van de Telecommunicatiewet:
- enhanced media service (EMS) en multimedia service (MMS) in de definitie van telefoondienst, in het eerste onderdeel a;
Onder B:
- e-mail over internet;
- internettelefonie onder B en de daarmee samenhangende toegewezen gebruikersidentificatie(s) en de gebruikersidentificatie of telefoonnummer van de beoogde ontvanger(s) van een internettelefoonoproep (sub a);
- datum en tijdstip van de log-in en log-off van een e-maildienst over het internet of internettelefoniedienst gebaseerd op een bepaalde tijdzone (sub e);
- het inbellende nummer voor een inbelverbinding (sub g);
- de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie (sub h).

Voorgesteld wordt om in de lijst van de te bewaren gegevens duidelijker tot uitdrukking te brengen dat telefonie via internet ook tot telefonie behoort, zodat helder is dat voor de te bewaren gegevens een bewaartermijn van twaalf maanden geldt. Er zijn VoIP-diensten waarvan de functionaliteiten zodanig nauw samenhangen met die van de traditionele telefonie dat deze diensten worden aangemerkt als telefonie over een vast of mobiel netwerk. Het gaat hier aldus niet om applicaties, zoals Skype of Facetime. Van belang is dat de functionaliteit en de gegenereerde gegevens overeen komen met die van een openbare telefoondienst. Voor dergelijke diensten zal een bewaartermijn van twaalf maanden gelden, in overeenstemming met de huidige regeling (Kamerstukken II, 2009/10, 32 185, nr. 3 en nr. 6, blz. 3 respectievelijk blz. 4). Hiervoor kan worden verwezen naar het «Standpunt eindgebruikersverplichtingen Voice over IP diensten» van de (toenmalige) Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) van 23 juni 2008[4].

Criteria die daarvoor van belang zijn:
- De VoIP-dienst is openbaar;

[4] www.acm.nl

- De VoIP-dienst kent de functionaliteit van in- en uitgaande gesprekken;
- De VoIP dienst maakt gebruik van het reguliere E.164 nummerplan.

Voor de verkeersgegevens van spraakdiensten die gebruik maken van het internet, en niet over deze functionaliteiten beschikken (zoals Skype en Facetime), geldt een bewaartermijn van zes maanden.

Verder blijken in de praktijk verschillende interpretaties van de term IP-adres, als bedoeld in de bijlage behorende bij artikel 13.2a, te bestaan. De bedoeling van de bewaarplicht voor telecommunicatiegegevens is dat gegevens beschikbaar zijn waarmee de abonnee of gebruiker van telecommunicatie kan worden geïdentificeerd. Als het begrip IP-adres te beperkt wordt uitgelegd, betekent dit dat slechts het interne IP-adres wordt opgeslagen zonder de daaraan gerelateerde gegevens zoals de poortnummers. Vanwege de technische ontwikkeling is een enkel intern IP-adres niet altijd tot een individuele gebruiker te herleiden maar kan, als de aanbieder Network Adress Translation (NAT) gebruikt, betrekking hebben op alle gebruikers in een straat of wijk. Dit strookt niet met het doel van de wet.
Voorgesteld wordt om de formulering aan te passen zodat expliciet tot uitdrukking komt dat IP-adressen, inclusief de datum en het tijdstip, in combinatie met de daaraan gerelateerde poortnummers moeten worden opgeslagen voor zover dit nodig is om de gebruiker te identificeren. Dat betekent dat aanbieders die gebruik maken van NAT of een vergelijkbare methodiek/techniek poortnummers moeten opslaan. Wanneer zij geen gebruik maken van NAT of een vergelijkbare techniek is het opslaan van poortnummers niet nodig. Op deze wijze wordt gewaarborgd dat IP-adressen, conform het doel van de wet, altijd te relateren zijn aan een gebruiker of abonnee. Dit betekent ook dat de opsporing gerichter kan plaatsvinden, hetgeen tot een beperktere inbreuk op de privacy leidt. Immers, als gericht gezocht kan worden naar een bepaalde abonnee of gebruiker behoeven andere gebruikers van hetzelfde IP-adres niet in beeld te worden gebracht.

Artikel II

Wijziging van het Wetboek van Strafvordering

Onderdeel A

Artikel 126n Sv

Derde en vierde lid
Het voorgestelde derde lid bevat een specifieke bepaling voor het vorderen van telecommunicatiegegevens, die door de aanbieders worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven. Deze bepaling vormt

een bijzondere regeling ten opzichte van de regeling voor het vorderen van verkeersgegevens, opgenomen in het eerste lid. Op grond van die regeling kan de officier van justitie, ingeval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten, in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker.

Met de voorgestelde bepaling worden nadere eisen gesteld aan het vorderen van telecommunicatiegegevens die door de aanbieders worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven. De nadere eisen betreffen de toegang tot de bewaarde gegevens en de voorafgaande machtiging van de rechter-commissaris.

De toegang tot de bewaarde telecommunicatiegegevens in verband met internettoegang en internettelefonie is afhankelijk van de ernst van het betreffende misdrijf. Daarbij wordt onderscheid gemaakt tussen misdrijven waarvoor voorlopige hechtenis mogelijk is en misdrijven waarvoor eveneens voorlopige hechtenis mogelijk is maar waarop tevens een gevangenisstraf van acht jaar of meer is gesteld. Bij verdenking van een strafbaar feit waarvoor voorlopige hechtenis kan worden opgelegd kunnen de bewaarde gegevens slechts worden geraadpleegd gedurende een periode van zes maanden voorafgaand aan de datum van de vordering. Bij verdenking van een feit waarvoor tevens gevangenisstraf van ten minste acht jaar of meer kan worden opgelegd kunnen de bewaarde gegevens worden geraadpleegd gedurende een periode van twaalf maanden voorafgaand aan de datum van de vordering. Concreet functioneert dit systeem als volgt. Stel dat de officier van justitie op 31 december een vordering richt tot een aanbieder tot verstrekking van telecommunicatiegegevens vanwege verdenking van het verleiden van een minderjarige tot ontucht (artikel 248a Sr). Voor een dergelijk misdrijf kan voorlopige hechtenis worden opgelegd. Dan kan de officier van justitie de telecommunicatiegegevens vorderen tot ten hoogste zes maanden voorafgaand aan de datum van de vordering. De officier kan dus een vordering doen ten aanzien van de gegevens die zijn vastgelegd tussen 1 juli en 31 december van dat jaar. De telecommunicatiegegevens die voor die datum zijn vastgelegd en die tijdens de periode waarop de vordering betrekking heeft op grond van de wettelijke bewaarplicht van twaalf maanden worden bewaard, worden door de aanbieder niet verstrekt. Als het zou gaan om verdenking van handel in kinderpornografie (artikel 240b, tweede lid, Sr), waarvoor naar de wettelijke omschrijving een gevangenisstraf van ten hoogste acht jaar is gesteld, dan kunnen de telecommunicatiegegevens worden gevorderd tot ten hoogste twaalf maanden voorafgaand aan de datum van de vordering, en dus over de periode vanaf 31 december van het jaar daarvoor tot aan de datum van de vordering. Voor de gegevens in verband met internettoegang en internettelefonie kunnen de bewaarde gegevens, ingeval van verdenking van een strafbaar feit waarvoor

ten minste voorlopige hechtenis kan worden opgelegd, gedurende de bewaartermijn van zes maanden worden geraadpleegd.

Met de verwijzing naar de gegevens, als bedoeld in het eerste lid, tweede volzin, onder a, wordt gedoeld op de zogenaamde historische verkeersgegevens. Dit betreft de verkeersgegevens die door de aanbieder zijn verwerkt ten tijde van de vordering tot verstrekking van de gegevens. De gegevens die op grond van het voorgestelde tweede lid, kunnen worden gevorderd, zijn beperkt tot de gegevens die in de bijlage behorende bij de Telecommunicatiewet zijn aangewezen. Van de historische verkeersgegevens kunnen worden onderscheiden de gegevens die na het tijdstip van de vordering worden verwerkt, de zogenaamd toekomstige verkeersgegevens. De vordering van toekomstige verkeersgegevens valt onder het eerste lid. De gegevens die op grond van het eerste lid kunnen worden gevorderd, zijn limitatief opgesomd in het Besluit vorderen gegevens telecommunicatie[5].

De vordering van de officier van justitie, op grond van dit lid, kan uitsluitend worden gericht tot de aanbieder die gehouden is tot de bewaring van de gegevens op grond van artikel 13.2a, tweede lid, van de Telecommunicatiewet. Deze kring van aanbieders is kleiner dan de kring van aanbieders, bedoeld in artikel 126la van het Wetboek van Strafvordering. Laatstgenoemde kring van aanbieders omvat tevens de aanbieders van niet-openbare bedrijfsnetwerken, communicatie faciliterende webdiensten en sociale netwerksites. Deze aanbieders dienen in beginsel uitvoering te geven aan vorderingen van de officier van justitie of de opsporingsambtenaar maar de verplichting tot bewaring van telecommunicatiegegevens, op grond van artikel 13.2a, tweede lid, van de Wet bewaarplicht telecommunicatiegegevens, is op hen niet van toepassing.

Vierde lid
De vordering van de officier van justitie, op grond van dit lid, kan uitsluitend worden gegeven na een voorafgaande machtiging van de rechter-commissaris. Op grond van de door de officier van justitie aan te voeren feiten en omstandigheden kan de rechter-commissaris besluiten tot de afgifte van een machtiging tot het raadplegen van de bewaarde telecommunicatiegegevens. Daarbij toetst de rechter-commissaris de wettelijke voorwaarden voor de vordering, zoals de aard en ernst van de verdenking, de ernst van het strafbare feit, waarvoor de gegevens worden gevorderd, de periode waarover de gegevens worden gevorderd en de proportionaliteit en subsidiariteit van de vordering. Voorgesteld wordt dat artikel 126l, zevende lid, van overeenkomstige toepassing is, zodat de machtiging bij dringende noodzaak, ingeval van spoed, mondeling kan worden gegeven. De rechter-commissaris stelt in dat geval de machtiging binnen drie dagen op schrift. Eenzelfde bepaling geldt voor het vorderen van

[5] Stb. 2004, 394.

gegevens betreffende de inhoud van een e-mailbericht, dat bij een internetaanbieder is opgeslagen (artikelen 126ng/ug, vierde lid, Sv).

Vijfde lid
Dit lid bevat de gegevens die in de vordering aan de aanbieder moeten worden vermeld. Dit betreft de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon over wie gegevens worden gevorderd en de gegevens die worden gevorderd. De officier van justitie zal in de vordering tevens de periode opnemen waarover de gegevens worden gevorderd, zodat het voor de aanbieder duidelijk is welke gegevens verstrekt moeten worden.

Zevende lid
In dit lid is vastgelegd dat artikel 126n, tweede, vierde en zesde lid, van toepassing is. Dit betreft de bescherming van het verschoningsrecht, de verplichting tot het opmaken van een proces-verbaal en de mogelijkheid om bij of krachtens algemene maatregel van bestuur nadere regels te stellen over de wijze waarop de gegevens door de officier van justitie worden gevorderd. De officier van justitie vermeldt in het proces-verbaal de gegevens die zijn opgesomd in artikel 126n, vierde lid, Sv. Voorgesteld wordt daaraan toe te voegen de periode waarover de vordering zich uitstrekt.

Onderdeel B

Artikel 126u

Derde lid
Dit lid bevat een specifieke bepaling voor het vorderen van telecommunicatiegegevens die door de aanbieders worden bewaard ten behoeve van het onderzoek naar georganiseerde criminaliteit.

Deze bepaling vormt een bijzondere regeling ten opzichte van de regeling voor het vorderen van verkeersgegevens, opgenomen in het eerste lid. Deze regeling vormt onderdeel van Titel V van het Wetboek van Strafvordering, waarin bijzondere opsporingsbevoegdheden zijn opgenomen die kunnen worden ingezet bij het onderzoek naar een georganiseerd verband waarin ernstige misdrijven worden beraamd of gepleegd. Op grond van die regeling kan de officier van justitie, in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker, indien uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven waarvoor voorlopige hechtenis is toegelaten worden beraamd of gepleegd die, gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren.

Voor de regeling van het vorderen van verkeersgegevens ten behoeve van het onderzoek naar georganiseerde criminaliteit is aangesloten bij de regeling van artikel 126n Sv. Ingeval van een redelijk vermoeden dat in georganiseerd verband ernstige strafbare feiten worden beraamd of gepleegd is de vordering van de gegevens beperkt tot het geval van een verdenking van ten minste een misdrijf waarvoor voorlopige hechtenis kan worden opgelegd. Daarbij is de toegang tot de bewaarde telefoniegegevens eveneens afhankelijk van de ernst van het betreffende misdrijf. Ingeval van een redelijk vermoeden dat in georganiseerd verband een strafbaar feit wordt beraamd of gepleegd waarvoor voorlopige hechtenis mogelijk is kunnen de gegevens slechts worden geraadpleegd die zijn bewaard gedurende een termijn van zes maanden voorafgaand aan de datum van de vordering. Ingeval van een redelijk vermoeden dat in georganiseerd verband een strafbaar feit wordt gepleegd waarvoor gevangenisstraf van tenminste acht jaar of meer kan worden opgelegd kunnen de telefoniegegevens worden geraadpleegd die zijn bewaard gedurende een periode van twaalf maanden voorafgaand aan de datum van de vordering. De vordering van de officier van justitie kan uitsluitend worden gegeven na een voorafgaande machtiging van de rechter-commissaris.

Onderdeel C

Dit betreft een wijziging van technische aard die voortvloeit uit de vernummering van het derde tot en met zesde lid van de artikelen 126n en 126u Sv tot respectievelijk het zesde tot en met negende lid, van de artikelen 126n en 126u Sv.

De Minister van Veiligheid en Justitie,