Openbaar Ministerie

College van Procureurs-Generaal

Voorzitter

Postbus 20305 2500 EH Den Haag

Prins Clauslaan 16
2595 AJ Den Haag
Telefoon +31 (0)70 339 96 00
telefax +31 (0)70 339 98 51

Ministerie van Veiligheid en Justitie

Postbus 20301
2500 EH DEN HAAG

| | |
|---|---|
| Onderdeel | WBOM |
| Contactpersoon | |
| Doorkiesnummer(s) | |
| E-mail | |
| Datum | 13 februari 2015 |
| Ons kenmerk | |
| Uw kenmerk | |
| Onderwerp | Advies conceptwetsvoorstel wijziging Telecommunicatiewet en het Wetboek van Strafvordering i.v.m. de bewaring van gegevens die zijn verwerkt i.v.m. met het aanbieden van openbare elektronische communicatiediensten |

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

Bij brief van 18 november 2014 heeft u namens de Minister van Veiligheid en Justitie het College van procureurs-generaal gevraagd te adviseren over een conceptwetsvoorstel, dat voorziet in een 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 dataretentie 2006/24/EG[1] ongeldig verklaard.
Het 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.

**Algemeen**

De samenleving is de afgelopen decennia ingrijpend gewijzigd. Naast wat tegenwoordig wel de fysieke of de analoge wereld wordt genoemd, is een nieuwe virtuele wereld ontstaan, het internet, inclusief de daarbij behorende digitale telecommunicatie. Een wereld die bestaat uit abstracte bits en bytes, maar die desalniettemin zeer reëel is. Belangrijke delen van ons sociale leven en de economie

[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)

hebben zich naar die virtuele wereld verplaatst. Veel economische activiteiten zijn onlosmakelijk verbonden met het gebruik van internet en zijn sterk afhankelijk van het internet en de moderne communicatiemiddelen. Die snelle ontwikkeling van telecommunicatie en internet is gepaard gegaan met de opkomst van nieuwe vormen van criminaliteit. Denk daarbij aan cybercrime, zoals internetoplichting en DDOS-aanvallen of een zedendelict als grooming. Deze vormen van criminaliteit laten nagenoeg uitsluitend op het internet hun sporen achter en zijn dan ook alleen op te sporen met behulp van het internet.
Meer klassieke vormen van criminaliteit worden in toenemende mate gepleegd met behulp van het internet en mobiele telecommunicatie. Denk daarbij aan misdrijven waarbij communicatie centraal staat, zoals stalking, verspreiding van kinderporno, bedreiging en de opruiing tot terroristische misdrijven.
Maar ook voor andere ernstige misdrijven waarbij ICT niet noodzakelijkerwijs als hulpmiddel is gebruikt, geldt dat de opsporing in toenemende mate afhankelijk is geworden van de beschikbaarheid van internet- en verkeersgegevens. In samenhang met klassieke opsporingsmethodieken kunnen deze gegevens sturing geven aan het onderzoek dan wel tot bewijs dienen.

Indien in de gewone wereld een misdrijf wordt gepleegd, dan kan onderzoek worden gedaan naar de fysieke sporen die de pleger van het misdrijf heeft achtergelaten. Zo kan op tastbare voorwerpen vingerafdrukken worden afgenomen, voetsporen veilig worden gesteld, bloedsporen worden onderzocht op DNA en eventuele getuigen kunnen worden ondervraagd. Zo niet bij de criminaliteit die wordt begaan op het internet of met behulp van het internet. In deze virtuele wereld bevinden de sporen zich vooral of uitsluitend in digitale vorm bij de aanbieders van telecommunicatie en de serviceproviders. Het wissen van verkeersgegevens kan ongeveer worden vergeleken met het afvegen van een vaas zodat vingerafdrukken niet meer aanwezig zijn, of het verwijderen van bloedsporen zodat DNA-onderzoek onmogelijk wordt. Zonder verkeersgegevens is de kans op een positieve identificatie van de pleger van het strafbare feit erg klein, immers, ook de sporen van het crimineel handelen bevinden zich veelal uitsluitend op het internet.

Het College heeft begrip voor het feit dat de wetgever een goede balans dient te zoeken tussen enerzijds de bescherming van de persoonlijke levenssfeer, het recht op privacy, en er anderzijds tegelijkertijd voor dient te zorgen dat de maatschappij wordt beschermd tegen ernstige criminaliteit. Want ook in een virtuele wereld is het een belangrijke taak van de overheid om ervoor te zorgen dat mensen zich daar veilig kunnen begeven en dat zij waar mogelijk worden beschermd tegen criminaliteit. Voorkomen moet worden dat een digitale vrijstaat ontstaat, waar zonder risico op vervolging en veroordeling strafbare feiten kunnen worden gepleegd. In dit verband is het goed dat het College nog eens wijst op de waarborgen waarmee de huidige Wet

bewaarplicht is omgeven. Zeker, het is waar dat de verkeersgegevens van alle burgers die communiceren via (mobiele) telefoons, tablets en computers tijdelijk worden opgeslagen. Maar deze gegevens worden niet bij de overheid opgeslagen, maar bij de aanbieders conform de eisen die bij wet en besluit zijn vastgelegd en waarop door middel van controles en anderszins wordt toegezien door het Agentschap Telecom. Politie en openbaar ministerie kunnen die gegevens niet '*at random*' bevragen en analyseren. Er is onder geen enkele omstandigheid sprake van data mining of profiling. Een bevraging is alleen mogelijk indien is voldaan aan de voorwaarden zoals die zijn opgenomen in het Wetboek van Strafvordering. Er moet — in het concrete, individuele geval — dus sprake zijn van de verdenking van een ernstig misdrijf. Verkeersgegevens worden alleen opgevraagd nadat in de concrete zaak een afweging is gemaakt tussen de privacy-schending en het belang van de opsporing en de officier van justitie van oordeel is dat de bevraging proportioneel is.
Uit reacties op de bewaarplicht blijkt dat soms het beeld bestaat dat ook de inhoud van de communicatie enige tijd wordt bewaard. Dat is beslist niet het geval. De gebruikers- en verkeersgegevens zijn de zogenaamde NAW-gegevens van telefoonnummers en IP-adressen. Het gaat om de gegevens waaruit blijkt wie op welk moment welk telefoonnummer of IP-adres in gebruik had. Verkeersgegevens telefonie laten zien welk nummer belde of sms'-te met welk ander nummer en waar. In geen geval wordt het bericht bewaard of wat iemand zegt. Van een IP-adres worden alleen de log-on en log-off gegevens bewaard. En dus beslist niet welke sites zijn bezocht, niet wat er is gegoogled, niet met wie is gecommuniceerd (skypen, chatten of whatsappen) en niet welke internetaankopen zijn gedaan. De inhoud van telefoongesprekken of de activiteit op het internet wordt niet geregistreerd.

**Het belang van de bewaarplicht**

Het College is verheugd dat het belang van dataretentie door de wetgever wordt onderkend. In de memorie van toelichting wordt op de pagina's 8 t/m 14 uitvoerig ingegaan op het belang van de bewaarplicht van verkeersgegevens voor de praktijk. Er wordt een aantal voorbeelden genoemd, waar het College graag nog een aantal opmerkingen aan toe wil voegen.
Genoemd wordt het vervolgonderzoek in de zaak Robert M., waarin de historische verkeersgegevens van groot belang zijn geweest om bewijs te verzamelen voor het grootschalig misbruik, maar ook om slachtoffers en medeverdachten in beeld te krijgen. Er wordt opgemerkt dat in 2011 de bewaartermijn voor internetgegevens nog twaalf maanden was. In deze zaak heeft het gebruik van de bewaarde gegevens geleid tot de aanhouding van meer dan honderdvijftig verdachten en zijn meer dan honderd kinderen uit een actuele misbruiksituatie gehaald. Terecht zegt de memorie van toelichting dat indien de bewaartermijn destijds, zoals nu het geval is, zes maanden was geweest, dit grote consequenties zou hebben gehad voor het identificeren van de

slachtoffers en medeverdachten. Het College zou graag duidelijk willen maken dat de consequentie zou zijn geweest dat het bij gebrek aan aanknopingspunten vrijwel onmogelijk was geworden om de andere verdachten aan te houden en dat er ernstig rekening mee moet worden gehouden dat de identificatie van de meer dan honderd kinderen in de misbruiksituatie ook niet mogelijk zou zijn geweest.

Het volgende in de memorie van toelichting gebruikte voorbeeld betreft een internationaal onderzoek naar kindermisbruik, waarin het buitenlandse opsporingsinstanties was het gelukt om zeer veel IP-adressen van gebruikers te achterhalen. In het bestand bevonden zich IP-adressen, die zouden kunnen worden gekoppeld aan meer dan honderd Nederlanders. Geen van deze zaken kon in behandeling worden genomen omdat de bewaartermijn was verlopen en dus de enige aanknopingspunten, te weten de IP-adressen, niet meer beschikbaar waren. Andere onderzoeksmogelijkheden ontbraken.
Dit is een veel voorkomend probleem bij uit andere landen komende rechtshulpverzoeken. Vanwege het tijdsverloop is Nederland in veel gevallen niet in staat om bij te dragen aan internationale onderzoeken, omdat de termijn voor de bewaarplicht al is verlopen. Bij gebrek aan andere onderzoeksmogelijkheden kan Nederland dan niet voldoen aan verzoeken om hulp van andere landen.

In het overzicht ontbreken voorbeelden van cybercrime en internetfraude. Dat is ten onrechte, want deze vorm van criminaliteit kan de samenleving ernstig ontwrichten. Bovendien zijn dit bij uitstek vormen van criminaliteit die zonder het voorhanden hebben van verkeersgegevens niet kunnen worden opgelost.
Zo is het voorgekomen dat een hacker is binnengedrongen in de infrastructuur van een grote communicatieaanbieder en daar enorme schade had kunnen toebrengen. De hacker is tijdig aangehouden kunnen worden, dankzij onderzoek aan de hand van historische gegevens van de gebruikte IP-adressen.
Voorts komt het tegenwoordig met enige regelmaat voor dat banken doelwit zijn van fraudeurs, die door middel van internetbankieren geld van de rekening van burgers trachten te halen. De bank is in dit geval de benadeelde, omdat die haar cliënt schadeloos stelt. In veel gevallen van fraude met internetbankieren is het IP-adres van de computer die door de verdachte is gebruikt het enige spoor. Indien de internetgegevens zijn vernietigd, is een strafrechtelijk onderzoek onmogelijk geworden. In een aantal gevallen is het onderzoek om die reden gestaakt.

In de memorie van toelichting wordt een aantal voorbeelden genoemd aan de hand waarvan het belang van het beschikbaar zijn van verkeersgegevens voor de praktijk wordt geduid. Deze voorbeelden kunnen moeiteloos met tientallen anderen worden aangevuld. De conclusie op pagina 14 van de memorie van toelichting, dat de opsporing 'is gebaat' bij mogelijkheden om telecommunicatiegegevens gedurende

langere tijd te bewaren en te gebruiken, is daarom naar het oordeel van het College aan de voorzichtige kant geformuleerd. Het belang van de bewaarplicht van verkeersgegevens voor de praktijk kan niet worden overschat. In de moderne opsporing is het voorhanden hebben van verkeersgegevens van telefonie en internet in toenemende mate bepalend voor het oplossen van de zaak. Er zijn tegenwoordig maar weinig moorden die worden opgelost zonder de hulp van verkeersgegevens.

Van het openbaar ministerie is de afgelopen jaren gevraagd om de opsporing en vervolging van ernstige internet gerelateerde criminaliteit te intensiveren. In de Veiligheidsagenda van de regering wordt een aantal speerpunten genoemd, waaronder de bestrijding van cybercrime en ernstige zedendelicten zoals de vervaardiging en verspreiding van kinderporno en grooming, waarvoor de Nationale Politie en het openbaar ministerie een extra inspanning zullen verrichten. Het College wijst tevens op het Actieprogramma Integrale Aanpak Jihadisme, waar in het kader van de bestrijding van terrorisme een groot aantal maatregelen en acties wordt aangekondigd om jihadgangers aan te kunnen pakken. Deelnemers aan de jihadistische beweging zijn bij uitstek personen die gebruik maken van moderne communicatiemiddelen en het internet.
Er gaan inmiddels stemmen op om de bewaarplicht voor verkeersgegevens in zijn geheel af te schaffen. De consequentie van een dergelijk besluit zou zijn dat politie en openbaar ministerie minder criminaliteit kunnen opsporen en vervolgen. In dat geval dient zelfs te worden aanvaard dat een belangrijk deel van de internet-gerelateerde criminaliteit in zijn geheel niet meer kan worden bestreden. Voor de bestrijding van al deze vormen van ernstige, in sommige gevallen zeer bedreigende criminaliteit geldt, dat het noodzakelijk is dat politie en justitie kunnen beschikken over de internet-verkeersgegevens. Het College is van oordeel dat met de aangekondigde intensivering van de bestrijding van terrorisme, cybercrime en ernstige zedendelicten niet is te verenigen dat tegelijkertijd de mogelijkheden om deze criminaliteit op te sporen en te vervolgen in ernstige mate worden beperkt of zelfs feitelijk onmogelijk wordt gemaakt.

De gevolgen van het beperken van het bewaren en gebruik van verkeersgegevens bij een herziening van de Wet bewaarplicht zijn aanzienlijk. Onderzoeken naar de klassieke vormen van criminaliteit, zoals moord en doodslag, of georganiseerde (drugs)criminaliteit, zullen langer duren en ook substantieel meer onderzoekscapaciteit gaan vergen. Bovendien zullen dan veel zwaardere bevoegdheden moeten worden ingezet om tot opsporingsindicaties te kunnen komen. Waar bijvoorbeeld het gebruik van verkeersgegevens uitsluitsel zou kunnen geven over de vraag welk telefoonnummer kan worden gelinkt aan een ander telefoonnummer (om zo bij een persoon uit te kunnen komen), zal een telefoontap moeten worden gebruikt, waarbij noodzakelijkerwijs de inhoud van de gesprekken wordt afgeluisterd.

Een telefoontap levert een grotere schending op van de privacy dan het gebruik van verkeersgegevens.
In een aantal gevallen zal het inzetten van zwaardere bevoegdheden ook geen soelaas bieden. De opsporing en vervolging van een belangrijk deel van de criminaliteit die op of door middel van het internet wordt gepleegd is alleen mogelijk indien de verkeersgegevens beschikbaar zijn.

Ten slotte vestigt het College met nadruk de aandacht op het belang van de slachtoffers. Vooral misdrijven die plaatsvinden in de persoonlijke levenssfeer, zoals geweldsdelicten en zedendelicten, grijpen diep in het leven van het slachtoffer. Voor deze slachtoffers is niets zo erg dan dat hun zaak niet wordt opgelost. En juist bij vormen van criminaliteit die een enorme persoonlijke impact op slachtoffers hebben, zoals stalking en bepaalde zedendelicten, hangt een succesvolle opsporing en vervolging grotendeels af van het beschikbaar hebben van verkeersgegevens. Terecht wordt in de memorie van toelichting de aandacht gevestigd op het belang van het beschikbaar zijn van verkeersgegevens voor het belang van de opsporing. Maar het College adviseert om tevens een paragraaf op te nemen die is gewijd aan het belang van het slachtoffer.

**Europees perspectief**

Ook vanuit het Europees perspectief gezien moet het mogelijk zijn dat een regeling wordt gecreëerd die enerzijds voldoende waarborgen biedt voor de eerbieding van de persoonlijke levenssfeer en anderzijds politie en justitie voldoende in staat stelt ernstige internet-gerelateerde criminaliteit te bestrijden. Dat het Hof van Justitie de Europese dataretentie richtlijn (2006/24/EG) ongeldig heeft verklaard omdat deze gebrekkig is opgesteld, wil nog niet zeggen dat de gedachte, de intentie, achter deze richtlijn er plotseling niet meer toe zou doen. Niet uit het oog mag worden verloren dat in Europa al heel lang aandacht bestaat voor de snelle ontwikkeling van telecommunicatietechnieken en het internet en het feit dat dit leidt tot de opkomst van nieuwe vormen van criminaliteit, dat de nieuwe technieken kunnen bijdragen aan het plegen van klassieke vormen van criminaliteit en dat gezocht moet worden naar een effectieve wijze van criminaliteitsbestrijding. De Raad van Europa heeft al in 1989 dit gevaar onderkend en het Comité van Ministers heeft in die tijd Recommendation No. R (89) 9 betreffende computercriminaliteit aangenomen.
En om te stimuleren dat de lidstaten ervoor zouden zorgen dat politie en justitie over voldoende onderzoeksbevoegdheden zouden kunnen beschikken heeft het Comité van Ministers in 1995 Recommendation No. R (95) aangenomen, betreffende verschillende problemen aangaande de strafvordering in verband met de informatiemaatschappij. Een van de aanbevelingen was, dat de lidstaten ervoor moesten zorgen dat 'speciale verplichtingen zouden moeten worden opgelegd aan service providers die

telecommunicatiediensten aanbieden aan het publiek om informatie te verschaffen om een gebruiker te identificeren in het geval dit zou worden gevraagd door de bevoegde onderzoeksautoriteit.'

Hiervoor is geschetst dat de opkomst van het internet en mobiele telecommunicatie ertoe heeft geleid dat nieuwe vormen van criminaliteit zijn ontstaan en dat klassieke vormen van criminaliteit nieuwe verschijningsvormen hebben gekregen, dan wel vergemakkelijkt zijn. En dat het logische gevolg daarvan is dat de opsporing van dergelijke ICT-gefaciliteerde delicten nauwelijks nog — of in een groot aantal gevallen in het geheel niet — mogelijk is, wanneer er geen bewaarplicht zou zijn.

Het valt op dat deze dimensie in de inleidende overwegingen bij de door het Hof van Justitie ongeldig verklaarde richtlijn nauwelijks aandacht krijgt. Er staat slechts een verwijzing naar een conclusie van de JBZ-Raad dat 'wegens de opmerkelijke toename van de mogelijkheden van elektronische communicatie, gegevens betreffende het gebruik daarvan van bijzonder belang zijn en een waardevol instrument bij het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, met name in de strijd tegen de georganiseerde misdaad' en dat 'gebleken is dat de bewaring van de gegevens een noodzakelijk en doeltreffend onderzoeksinstrument is voor wetshandhaving in verschillende landen.'[2]

Die vanuit het belang van de rechtshandhaving anno 2015 veel te abstracte en te beperkte onderbouwing van de noodzaak van dataretentie lijkt door te werken bij de toetsing van de richtlijn door het Hof van Justitie aan (o.a.) het EU-handvest.
Het Hof overweegt onder meer dat 'de gegevens die op grond van deze richtlijn moeten worden bewaard, gelet op het groeiende belang van elektronische communicatiemiddelen de nationale strafvervolgingsautoriteiten extra mogelijkheden bieden om ernstige gevallen van criminaliteit op te helderen en in die zin dus een waardevol instrument vormen bij strafonderzoeken.'[3] Waar het de noodzaak van de dataopslag betreft concludeert het Hof dat 'de doeltreffendheid van de bestrijding van zware criminaliteit in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel, zoals die welke door richtlijn 2006/24, noodzakelijk wordt geacht voor het voeren van deze strijd.'[4]

---

[2] Richtlijn 2006/24/EG van 15 maart 2006, overweging 7, resp. 9, uit de considerans.

[3] R.o. 49.

[4] R.o. 51.

Het Hof is bij de beoordeling van de evenredigheid van de maatregel kennelijk vooral af gegaan op de summiere, bijna plichtmatige onderbouwing uit de richtlijn. Het gegeven dat belangrijke onderdelen van de moderne criminaliteit zonder dataretentie niet of slechts bij uitzondering kan worden opgespoord en vervolgd lijkt geen rol te hebben gespeeld in de overwegingen in de overwegingen van het Hof.

Het is maar de vraag of het Hof van Justitie bij de afweging tussen enerzijds het belang van de bescherming van de persoonlijke levenssfeer en anderzijds het belang van de openbare veiligheid en de strafrechtelijk handhaving, dat laatste belang net zo makkelijk had weggewuifd als in het arrest van 8 april 2014 is gebeurd wanneer in de toelichting op de richtlijn scherper was gesteld en onderbouwd dat zonder dataretentie strafrechtelijke handhaving voor een groot (en nog steeds) groeiend aantal misdrijven eenvoudigweg onmogelijk is.

In dat verband kan er ook op worden gewezen dat de EU zelf regelmatig de lidstaten aanspoort om strafrechtelijk op te treden op terreinen waar die handhaving feitelijk niet mogelijk is zonder dataretentie. Recente voorbeelden zijn de Richtlijn 2011/92 van 13 december 2011 van het Europees parlement en de Raad ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie en de richtlijn 2013/40/EU van het Europees Parlement en de Raad over aanvallen op informatiesystemen.

Ook in de Europese rechtspraak is terug te vinden dat lidstaten zorg dienen te dragen voor een effectieve criminaliteitsbestrijding. Het Europese Hof voor de Rechten van de Mens heeft expliciet bepaald dat het recht op privacy niet absoluut is, en dat de Lidstaten verplicht zijn een goede balans te vinden tussen privacybescherming en criminaliteitsbestrijding. In een arrest uit 2008 veroordeelde het EHRM Finland, omdat het naar Fins recht niet mogelijk was om de identiteit van een internetgebruiker te achterhalen. In dit geval ging het om een onbekende internetter die (zonder diens medeweten of toestemming) een seksuele advertentie op het internet heeft gezet voor een 12-jarige jongen, die vervolgens door een pedofiel werd benaderd. Het EHRM oordeelde dat Finland de plicht had zijn burgers tegen zulke strafbare feiten te beschermen en daarom wetgeving tot stand had moeten brengen waarbij enerzijds het recht op respect voor het privéleven van internetgebruikers en anderzijds het voorkomen en bestrijden van misdrijven met elkaar in evenwicht waren gebracht. Nederland is het derhalve verplicht aan zijn burgers die slachtoffer worden van ernstige misdrijven om daar effectief tegen op te treden.
W.N. Ferdinandusse concludeert in dit verband dat het bij de afweging van belangen niet zozeer gaat om de bescherming van burgers tegen een alwetende overheid, maar

dat het gaat om conflicterende belangen van burgers onderling (privacy versus bescherming tegen criminaliteit) en om conflicterende internationale verplichtingen.[5]

**Het wetsvoorstel**

A. *Gestaffelde toegang tot gegevens die moeten worden bewaard op grond van de Telecommunicatiewet.*

Voorgesteld wordt dat de bewaartermijn voor de gegevens met betrekking tot telefonie over een vast of mobiel netwerk wordt vastgesteld op twaalf maanden. De gegevens worden bewaard door de aanbieders en bevinden zich feitelijk nog niet bij de politie of het openbaar ministerie. Om de toegang tot de gegevens te verkrijgen is een vordering van de officier van justitie vereist. De bewaartermijn van twaalf maanden kan echter, anders dan tot nu toe, door de officier van justitie alleen worden benut wanneer sprake is van de zwaarste categorie delicten, waarop een strafdreiging is gesteld van acht jaar gevangenisstraf of meer. Bij lichtere delicten, waarvoor voorlopige hechtenis kan worden opgelegd maar waarop geen strafdreiging van acht jaar of meer is gesteld, mogen de gegevens slechts gedurende een periode van zes maanden worden gevorderd. 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.

Het College vraagt zich af waarom dit onderscheid wordt gemaakt. In de memorie van toelichting ontbreekt een nadere toelichting. Wel wordt gesteld dat dit een nieuwe aanvullende maatregel betreft, waarmee een zorgvuldige omgang met de bewaarde telefoniegegevens wordt beoogd. Het College is echter van oordeel dat de voorgestelde maatregel niet bevorderlijk is voor een zorgvuldig strafvorderlijk onderzoek. Het onderscheid tussen een delict waar vier jaar gevangenisstraf op is gesteld, of een delict waar acht jaar gevangenisstraf op is gesteld, is in veel gevallen in het beginstadium van het onderzoek niet goed te maken. Bij het vorderen van gegevens in een opsporingsonderzoek staat niet altijd bij voorbaat vast hoe de feiten waarvan men wordt verdacht kunnen worden gekwalificeerd. Om het in de memorie van toelichting gegeven voorbeeld van kinderporno te gebruiken: een persoon wordt verdacht van het bezit en verspreiden van kinderporno, strafbaar gesteld bij artikel 240b, eerste lid, Sr. Pas later kan uit het onderzoek blijken dat deze persoon van het plegen van dit delict een beroep of gewoonte heeft gemaakt. Gaandeweg het opsporingsonderzoek kunnen er (juist ook door de analyse van de verkeersgegevens) ernstiger feiten bijkomen

[5] NRC-Handelsblad , 15 januari 2015, W.N. Ferdinandusse: Charlie Hebdo toont belang bewaarplicht telecomgegevens

waarop een hoger strafmaximum is gesteld. Dit komt vaak voor bij de verdenking van zedendelicten. Omgekeerd kan de analyse van de verkeersgegevens ook tot de uitkomst leiden dat de verdenking kan worden beperkt tot feiten waarop een strafmaximum van vier jaar is gesteld, of kan de betrokkenheid bij strafbare feiten zelfs geheel worden uitgesloten.

In het systeem van strafvordering is de voorgestelde constructie een vreemde eend in de bijt. Er is maar één artikel in het Wetboek van Strafvordering waarin sprake is van de uitoefening van een bevoegdheid, waarbij als voorwaarde wordt gesteld dat er sprake moet zijn van een verdenking van een strafbaar feit waarop acht jaar of meer gevangenisstraf is gesteld en dat is artikel 126l, tweede lid, Sv.[6] Dat betreft de bevoegdheid om ter uitvoering van een bevel opnemen vertrouwelijke communicatie een woning binnen te treden zonder toestemming van de bewoner teneinde de benodigde apparatuur te plaatsen. Maar dan is het onderwerp van de bevoegdheid ook een zeer op de persoonlijke levenssfeer ingrijpende bevoegdheid. Want met deze bevoegdheid wordt beoogd om zonder medeweten van de verdachte apparatuur in zijn woning te plaatsen, teneinde gesprekken af te luisteren en de inhoud van deze gesprekken te betrekken in het strafrechtelijk onderzoek. Het gebruik maken van gevorderde verkeersgegevens, het onderwerp van het onderhavige wetsvoorstel, staat in geen enkele verhouding tot deze bevoegdheid.

Het College is voorts geen voorstander van de gestaffelde toegang tot de bewaarde gegevens omdat in het geval van een strafrechtelijk onderzoek in veel gevallen zal worden gekeken of de verdenking voor een zwaarder delict mogelijk is, teneinde over een langere periode gegevens te kunnen vorderen. Dat is noodzakelijk, want eenmaal gekozen voor een lichter feit is het daarna, gelet op het tijdsbeslag van het onderzoek, praktisch niet meer mogelijk om gegevens te vorderen die langer dan zes maanden zijn bewaard.
Bovendien is te voorspellen dat, net zoals dat in het verleden bij de voorlopige hechtenis is gebeurd, in de toekomst op een aantal delicten een hogere gevangenisstraf wordt gesteld dan men vanuit het oogpunt van gerechtvaardigde straf noodzakelijk acht, alleen maar om mogelijk te maken dat de opsporingsinstanties kunnen beschikken over gegevens die tot twaalf maanden worden bewaard.

---

[6] Ook in de artikelen 226g en 481 Sv is sprake van een misdrijf waarop meer dan acht jaar gevangenisstraf is gesteld. Dit betreft echter geen verdenking van een dergelijk feit, maar een afspraak over een gepleegd feit waarop acht jaar of meer is gesteld respectievelijk een veroordeling voor een strafbaar feit waarop acht jaar of meer is gesteld.

*B. Toetsing rechter-commissaris*

Voorgesteld wordt dat de officier van justitie de verkeersgegevens kan vorderen, maar dat de vordering slechts kan worden gedaan na voorafgaande door de RC te verlenen schriftelijke machtiging. Om een aantal redenen maakt het College bezwaar tegen de voorgestelde regeling.

In de memorie van toelichting wordt gesteld dat 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. Het College vraagt zich echter af of het arrest noodzaakt tot de inzet van de RC. Zeker, er is een rechtsoverweging in het arrest waarin het Hof constateert dat de gewraakte datarichtlijn geen voorschriften bevatte met betrekking tot de bemoeienis van een rechter of een andere onafhankelijke autoriteit. Het College meent echter dat deze overweging moet worden gezien in het samenstel van overwegingen die het Hof tot de conclusie hebben doen leiden dat de richtlijn ongeldig is. Heel wel is voorstelbaar dat in het geval de richtlijn voldoende overige concrete waarborgen zou hebben bevat, het Hof deze overweging niet zou hebben opgenomen.
Nu de toets door de RC niet rechtstreeks is te herleiden tot een eis van het Hof moet de vraag worden gesteld naar de toegevoegde waarde van de toetsing door de RC in deze gevallen. Zowel de bewaring van de verkeersgegevens, de eisen die daaraan zijn gesteld, als het toezicht daarop zijn wettelijk geregeld. Hetzelfde geldt voor het gebruik van gegevens. Alleen in het geval dat een verdenking van een bepaald strafbaar feit bestaat, mag de officier van justitie de gegevens vorderen. Gesteld wordt dat door de beoordeling van de RC kan worden verzekerd dat de gegevens uitsluitend worden geraadpleegd in de gevallen waarin daartoe voldoende aanleiding bestaat.
De toets van de RC is echter, gegeven de omstandigheden waaronder de verkeersgegevens worden gevorderd, noodzakelijkerwijs beperkt tot de vraag of aan de wettelijke voorwaarden wordt voldaan. Een echte belangenafweging is in dit stadium niet mogelijk. Dat maakt de RC kwetsbaar. Indien de omstandigheden aanwezig zijn (gepleegde feit, verdenking) en het bevel wordt voor een correcte periode door de bevoegde autoriteit afgegeven, kan de RC niet veel anders doen dan de machtiging afgeven. De toets van de RC kan dus vanuit het oogpunt van rechtsbescherming geen bijzondere meerwaarde opleveren waar het gaat om de beoordeling van de rechtmatigheid van de vordering verkeersgegevens.

Tevens wordt gesteld dat de voorgestelde voorafgaande machtiging van de RC goed past in het wettelijk systeem van de inzet van bijzondere opsporingsbevoegdheden. Dat bestrijdt het College. Dat een voorafgaande machtiging van de RC voorkomt in het

Wetboek van Strafvordering wil nog niet zeggen dat de voorgestelde constructie past in het wettelijk systeem. In die zin is het net zo'n vreemde eend in de bijt als de voorgestelde gestaffelde toegang tot gegevens. Het College wijst erop dat in het Wetboek van Strafvordering ingrijpende bijzondere bevoegdheden tot opsporing zijn opgenomen (infiltratie, stelselmatige observatie, stelselmatig inwinnen van informatie), die een grotere inbreuk op de privacy van betrokkenen met zich meebrengen en die zonder machtiging van de RC op bevel van de officier van justitie kunnen worden ingezet. Het invoeren van een toets door de RC voor het vorderen van niet-inhoudelijke gegevens, hetgeen een veel geringere inbreuk op de privacy maakt dan de overige opsporingsbevoegdheden, is een breuk met het systeem dat met de Wet bijzondere opsporingsbevoegdheden en de Wet vorderen gegevens vorm heeft gekregen.

Voorts merkt het College op dat het voorstel in de praktijk tot grote problemen zal leiden. Afgemeten aan de gegevens over 2013 is de schatting dat ruim 46.000 vorderingen per jaar extra aan de RC zullen moeten worden voorgelegd. Dat zal ongetwijfeld tot grote vertragingen leiden, gelet op de huidige belasting van de kabinetten-RC. Vertragingen bij de behandeling van de vordering van verkeersgegevens zal ertoe leiden dat deze gegevens in toenemende mate niet meer beschikbaar zijn.
Ook leidt dezelfde RC-toets er toe dat bij de uitvoering van rechtshulpverzoeken waarin om verkeersgegevens wordt gevraagd (ruim duizend gevallen op jaarbasis) er een verlofprocedure (ex art. 552p Sv) moet worden gevolgd voordat de gegevens aan het buitenland kunnen worden verstrekt. Te voorzien is dat een groot aantal extra raadkamerzittingen moet worden gepland. De vertraging in de behandeling en de daaropvolgende vertraging in het vervolg van het opsporingsonderzoek in het buitenland die dit zal opleveren, kan flinke druk zetten op de rechtshulprelatie met het buitenland.

Alles afwegende adviseert het College om de voorgestelde voorafgaande machtiging van de RC te schrappen. Het is niet noodzakelijk, de toegevoegde waarde van de toets door de RC is gering en de kosten en de praktische problemen voor de praktijk waarmee dit voorstel gepaard zal gaan zijn substantieel.
Het College is op zichzelf voorstander van een meer actieve rol van de RC bij de opsporing en vervolging. Maar het College meent dat dit beter kan worden geregeld bij een integrale herziening van de rol van de RC in het kader van de modernisering van het Wetboek van Strafvordering. Bij die gelegenheid kan de taak en rol van de RC tegen het licht worden gehouden bij het toezicht op alle bevoegdheden van politie en officier van justitie, waarbij de verschillende bevoegdheden in onderling verband kunnen worden bezien.

*C. Technische opmerkingen*

**Artikel 13.2a Telecommunicatiewet**

Het tweede lid van artikel 13.2a wordt gewijzigd. De huidige formulering "ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven" wordt vervangen door "teneinde te kunnen voldoen aan een vordering op grond van artikel 126n, artikel 126u of artikel 126zh van het Wetboek van Strafvordering".
Met de wijziging wordt beoogd het doel van de bewaring preciezer te omschrijven en een objectief criterium te bieden ter begrenzing van de toegang van de bevoegde autoriteiten.
Het College wijst erop dat de bewaarde gegevens ook mogen worden gebruikt om te voldoen aan de vorderingen ingevolge de artikelen 126na en 126ng Sv en de overeenkomstige bepalingen in Titel V en Titel VI. Bij de voorgestelde constructie zouden deze artikelen in ieder geval aan het tweede lid van artikel 13.2a moeten worden toegevoegd.

Meer in het algemeen merkt het College op dat in de Telecommunicatiewet in verschillende bepalingen de verplichting is opgenomen aan een vordering van de officier van justitie te voldoen. De plicht om aan de vordering te voldoen vloeit echter niet voort uit de Telecommunicatiewet, maar uit het Wetboek van Strafvordering. Een ieder is verplicht om te voldoen aan de vordering of het bevel indien deze rechtmatig is gegeven door de bevoegde autoriteit, te weten de officier van justitie.[7] Niet voldoen aan een vordering of bevel, krachtens wettelijk voorschrift gedaan door een ambtenaar die is belast met of bevoegd verklaard tot het opsporen van strafbare feiten, levert ingevolge artikel 184 Sr bovendien een strafbaar feit op.
Er is geen enkele andere wet waarin een vergelijkbare verplichting is opgenomen. Het College meent dat de verplichting voor de aanbieders in de Telecommunicatiewet om te voldoen aan een rechtmatig gegeven bevel of vordering onnodig is en ten onrechte de indruk wekt dat in overige gevallen niet aan een rechtmatig gegeven vordering of bevel hoeft te worden voldaan. Om die reden vraagt het College zich af of de betreffende bepalingen tegen het licht moeten worden gehouden teneinde te bezien of deze verplichting moet worden geschrapt.

---

[7] Dat het Wetboek van Strafvordering uitgaat van een verplichting blijkt uit het feit dat in de daarvoor in aanmerking komende gevallen *de afwezigheid van de verplichting* als uitzondering is geëxpliciteerd. Zie in dit verband artikel 98a, derde lid, Sv. Laatstgenoemde bepaling wordt van overeenkomstige toepassing verklaard in diverse Sv-artikelen die op het vorderen van gegevens betrekking hebben.

Het derde lid van artikel 13.2a wordt niet gewijzigd. Het College merkt echter op dat het de bedoeling is dat gegevens in verband met internettelefonie 12 maanden zullen worden bewaard. Deze kunnen ingevolge het voorgestelde derde lid, onderdeel b, van artikel 126n Sv worden opgevraagd in geval van een verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld. De internettelefonie zal dan in het derde lid, onderdeel b, van artikel 13.2a Telecommunicatiewet moeten worden geschrapt en expliciet moeten worden opgenomen in het derde lid, onderdeel a van artikel 13.2a.

**Bijlage behorende bij artikel 13.2a Telecommunicatiewet**

Onder nummer 5 wordt voorgesteld: "in onderdeel B komt onderdeel c (nieuw) te luiden:
c. Het IP-adres (inclusief datum en tijdstip), etc. ..."
Het College merkt op dat het noodzakelijk is dat duidelijk is om welke datum en tijdstip het gaat. Het College adviseert om de woorden "log on en log off" in te voegen na "tijdstip".

**Artikel 126n Wetboek van Strafvordering**

Op basis van de geldende wettelijke regeling is de situatie ontstaan dat een vordering aan een aanbieder van een communicatiedienst tot het verstrekken van andere gegevens dan verkeersgegevens mondeling kan worden gedaan. Voor een vordering tot het verstrekken van verkeersgegevens op grond van de artikelen 126n en 126u Sv is dit echter niet mogelijk. Dit levert in de praktijk regelmatig problemen op. Om die reden is besloten om bij gelegenheid van het wetsvoorstel Computercriminaliteit III deze omissie te repareren door voor te stellen om voor de bevoegdheid van het vorderen van verkeersgegevens door de officier van justitie expliciet de mogelijkheid te bieden van een mondelinge vordering van verkeersgegevens. In geval van een mondelinge vordering stelt de officier van justitie de vordering achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht.
De huidige situatie levert in de praktijk problemen op, maar tot op zekere hoogte is er wel mee te werken. Door analoog aan vergelijkbare artikelen te redeneren, zoals artikel 126nd, en te stellen dat het gaat om een kennelijke omissie van de wetgever kan in de meeste gevallen degene tot wie de vordering is gericht wel worden bewogen te voldoen aan een mondeling bevel van de officier van justitie. Echter, in het nu voorliggende wetsvoorstel wordt in artikel 126n, lid 4, de RC de mogelijkheid geboden de

machtiging mondeling te geven. Dat zal het voor de praktijk vrijwel onmogelijk maken nog aan de hand van een vergelijkbare bepaling een mondelinge vordering te geven." Immers, voor de RC zal de mondelinge machtiging dan expliciet in artikel 126n zijn vermeld.
Het is niet denkbeeldig, gelet op de discussies die over beide wetsvoorstellen mogelijk zijn, dat het onderhavige wetsvoorstel eerder in werking kan treden dan het wetsvoorstel Computercriminaliteit III. In dat geval kan de onwenselijke situatie ontstaan, dat in het geval de grootste spoed is vereist en de vordering mondeling moet worden gedaan, dit niet meer mogelijk is. Dat heeft grote consequenties voor de opsporingspraktijk. In veel gevallen gaat het plaatsen van een spoedtap, welk bevel ingevolge artikel 126m in verbinding met 126l en 126g Sv mondeling wordt gegeven, vergezeld van een mondelinge vordering verkeersgegevens. Dit zogenoemde combibevel, dat dagelijks in de praktijk wordt gegeven, is dan niet meer mogelijk. Het College adviseert dringend om de wijziging zoals die al is opgenomen in het conceptwetsvoorstel Computercriminaliteit III, over te hevelen naar het onderhavige wetsvoorstel.

**Artikel 577be Sv**

Het wetsvoorstel voorziet niet in een wijziging van artikel 577be Sv. Het College merkt op dat de voorgestelde wijziging van artikel 126n tevens noopt tot aanpassing van artikel 577be Sv.

Hoogachtend,
Het College van procureurs-generaal