BCPA

Ministerie van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken

Postbus 20301
2500 EH Den Haag

Amsterdam, 30 januari 2015

Betreft: *Bewaarplicht; uw brief van 18 november 2014 (kenmerk: 525682)*

Geachte heer Mol Lous,

Hierbij dien ik namens BCPA een zienswijze in naar aanleiding van het conceptwetsvoorstel tot wijziging van - kort gezegd - de bewaarplicht.

BCPA is een samenwerkingsverband van de in Nederland actieve dochterondernemingen van BT Group, Verizon Enterprise Solutions en Colt Technology Services. Deze aanbieders leveren wereldwijd netwerk- en IT-oplossingen aan multinationals, overheidsinstellingen en grote ondernemingen.

BCPA kan het voorliggende wetsvoorstel niet steunen. De juridische basis is wankel en de wet is dus kwetsbaar. BCPA ziet geen rechtvaardiging voor aanvullende verplichtingen en extra kosten, zeker niet uit hoofde van een kwetsbare wet.

Deze zienswijze belicht allereerst de bescheiden rol die grootzakelijke aanbieders spelen ter ondersteuning van de opsporing van strafbare feiten. Vervolgens bespreken wij het oordeel van het Hof van Justitie[1] en het advies van de Raad van State[2]. De conclusie van deze zienswijze is dat intrekking van dit wetsvoorstel onontkoombaar is, vanwege strijd met grondrechten van de Europese Unie en de belemmering van het vrij verkeer van diensten. BCPA pleit voor een vrijstelling van de verplichtingen uit hoofdstuk 13 Tw. Wij bespreken tenslotte nog de onwenselijke en onnodige eis dat de betrokken gegevens binnen de Unie moeten worden bewaard en verwerkt.

De rol van grootzakelijke aanbieders in het kader van de opsporing

Noch bij de invoering van de bewaarplicht, noch op enig moment nadien, is een kosten-batenanalyse gemaakt. BCPA durft niettemin de stelling aan dat de kosten die grootzakelijke aanbieders moeten maken om te voldoen aan de bewaarplicht niet in verhouding staan tot de baten die hiertegenover kunnen worden ingeboekt. Grootzakelijke aanbieders kunnen weinig bijdragen aan de opsporing en vervolging van strafbare feiten. De aard van hun dienstverlening brengt met zich mee dat BT, Colt en Verizon een zeer geringe hoeveelheid tapverzoeken te verwerken krijgen, veel minder dan de 'grote zes' aanbieders en vermoedelijk ook veel minder dan kleinere consumenten aanbieders. Grootzakelijke aanbieders worden niet of nauwelijks bevraagd op gegevens die verplicht moeten worden bewaard op grond van artikel 13.2a Tw. Op dit gebied zijn zij dus in feite 'kleine aanbieders'. Niettemin zijn de verplichtingen op grond van hoofdstuk 13 Tw. onverkort van toepassing op grootzakelijke aanbieders, met alle kosten van dien.

---

[1] Hof van Justitie van de Europese Unie te Luxemburg, 8 april 2014, arrest in gevoegde de zaken C-293/12 en C-594/12

[2] No.W03.14.0161/II/Vo 's-Gravenhage, 17 juli 2014

Van een evenwichtige vergoedingstructuur is nog steeds geen sprake. BCPA is alleen al om die reden van meet af aan kritisch geweest ten aanzien van de bewaarplicht, en ten aanzien van alle overige verplichtingen uit hoofdstuk 13 Tw.

Hof van Justitie en Raad van State

Het belangrijkste bezwaar tegen het conceptwetsvoorstel is dat het op essentiële punten voorbij gaat aan de uitspraak van het Hof van Justitie en aan het advies van de Raad van State. In weerwil van het oordeel van het Hof blijft de regering van mening dat de bewaring van gegevens van *alle* burgers noodzakelijk is. Het conceptwetsvoorstel omschrijft niet precies welke categorieën gegevens, van welke elektronische communicatiemiddelen, van welke personen strikt noodzakelijk zijn voor het voorkomen, opsporen of vervolgen van ernstige criminaliteit. Het Hof oordeelt dat er een verband moet bestaan tussen het gedrag van de personen van wie gegevens worden opgeslagen en zware criminaliteit. Dit verband is afwezig in het conceptwetsvoorstel. Ook de door het Hof geformuleerde voorwaarde, dat per categorie gegevens duidelijk en precies omschreven wordt voor welke periode het strikt noodzakelijk is dat die gegevens door telecommunicatie-aanbieders worden bewaard, is niet vervuld. Het Hof verlangt dat er bij de bewaartermijn onderscheid wordt gemaakt tussen de verschillende categorieën gegevens naargelang van het nut voor het nagestreefde doel en naargelang van de betrokken personen, en dat de bewaartermijn wordt vastgesteld op basis van objectieve criteria. Een dergelijk onderscheid ontbreekt in het conceptwetsvoorstel. Naar het oordeel van de Raad van State volgt uit het arrest dat in de nationale wetgeving aan alle afzonderlijke waarborgen, zoals genoemd door het Hof, moet worden voldaan. De regering volgt dit advies niet op.

Nu het wetsvoorstel grotendeels voorbij gaat aan het oordeel van het Hof en aan het advies van de Raad van State is de conclusie onontkoombaar

dat de juridische basis van het wetsvoorstel uiterst wankel is[3]. De regering handhaaft voorschriften die strijdig zijn met een hogere regeling en die mitsdien onverbindend zijn, waardoor het onrechtmatig overheidshandelen voortduurt. De regering zet de deur wijd open voor nieuwe procedures. Aanpassingen niet zullen volstaan. Het voorstel moet van tafel.

Vrij verkeer van diensten

Er dreigt bovendien een lappendeken van verschillende bewaarplichten te ontstaan binnen de Europese Unie. BCPA meent dat de Nederlandse regering niet op de muziek vooruit moet lopen met een nationale regeling. Het wetsvoorstel is een nationale wetgevingsmaatregel die telecommunicatie-aanbieders verplicht om apparatuur aan te schaffen en personeel in dienst te hebben om aan de bewaarplicht te kunnen voldoen. Daarmee vormt de maatregel een belemmering van het vrij verkeer van diensten (vgl. het advies van de Raad van State, pagina 6 tot en met 8). Als de overheid al wil vasthouden aan een bewaarplicht dient deze geharmoniseerd te worden ingevoerd binnen de Europese Unie, op een wijze die verenigbaar is met het vrij verkeer van diensten en met de grondrechten van de Europese Unie. Internationaal opererende aanbieders, zoals BT, Colt en Verizon, zijn niet gebaat bij verschillende regimes in verschillende lidstaten. Het huidige voorstel past niet binnen het streven naar harmonisatie van wetgeving, en moet ook om die reden worden afgewezen.

---

[3] Vgl. NRC Handelsblad d.d. 26 november jl., *Opstelten slaat onwettig onze data op | Bij opslag van kentekens en internetverkeer negeert de regering het Europese Hof*, door Prof. mr. E.J. Dommering en Prof. N.A.N.M. Van Eijk.

Vrijstelling voor 'kleine aanbieders'

Te vrezen valt echter dat de regering het wetsvoorstel niet zal intrekken. In dat geval pleit BCPA voor een vrijstelling voor 'kleine aanbieders' van de verplichtingen uit hoofdstuk 13 Tw. Een dergelijke vrijstelling bestaat reeds in het Verenigd Koninkrijk. In het Verenigd Koninkrijk zijn uitsluitend daartoe aangewezen aanbieders verplicht om gegevens op te slaan. Aanbieders die worden aangewezen worden gecompenseerd in de kosten.

Artikel 13.5 derde lid Tw.

Voor het geval dat een vrijstelling niet wordt verleend staat BCPA graag stil bij een enkel onderdeel uit het wetsvoorstel. Dit betreft de verplichting om de gegevens te bewaren en te verwerken in Nederland of in een andere lidstaat van de Europese Unie (artikel 13.5 lid 3 Tw). Deze verplichting dwingt aanbieders die de opslag en verwerking van gegevens (deels) buiten de Europese Unie laten plaatsvinden hun processen ingrijpend te wijzigen, met alle kosten van dien. Dit is hoogst onwenselijk. Wat de verwerking betreft dwingt de uitspraak van het Hof van Justitie niet tot deze verplichting. Het Hof overweegt in punt 68 het volgende:

> *In de tweede plaats schrijft deze richtlijn niet voor dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard, zodat niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de (...) vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest.*

Het Hof benadrukt dat de betrokken gegevens moeten worden *bewaard* op het grondgebied van de Unie, opdat het vereiste toezicht mogelijk is. Het Hof spreekt nergens over het *verwerken* van de betrokken gegevens op het grondgebied van de Unie. Hier gaat het wetsvoorstel verder dan het Hof, zonder enige motivering. Wel schrijft de regering op pagina 22 van de Memorie van Toelichting dat deze verplichting waarborgt dat de

opslag en verwerking voldoet aan de Europese normen op het gebied van de bescherming en beveiliging van de bewaarde gegevens. Deze verplichting beoogt een minimumniveau voor de gegevensbescherming en -beveiliging te waarborgen. Deze extra waarborg ten aanzien van de verwerking is echter overbodig. Immers, de Wet bescherming persoonsgegevens bevat reeds een verbod om persoonsgegevens door te geven naar landen buiten de Europese Unie die geen passend beschermingsniveau waarborgen (vgl. artikel 76 lid 1 Wbp en artikel 25 lid 1 van de Privacyrichtlijn 95/46/EG). Een passend beschermingsniveau is dus al gewaarborgd. Toch worden aanbieders die persoonsgegevens (deels) buiten de Unie verwerken straks gedwongen om deze praktijk ongedaan te maken, zelfs wanneer de verwerking plaatsvindt in een land met een passend beschermingsniveau. In dat geval voegt de verplichting dus niets toe, maar leidt deze verplichting slechts tot extra kosten. De woorden 'en verwerkt' dienen te worden geschrapt uit artikel 13.5 lid 3 Tw.

Wat de opslag van de gegevens betreft geldt eveneens dat extra waarborgen overbodig zijn. BCPA ziet niet goed waarom gegevens niet bewaard zouden mogen worden in landen buiten de Europese Unie, indien en voorzover daarbij een passend beschermingsniveau gewaarborgd wordt. De vrijheid van aanbieders moet niet onnodig worden ingeperkt. Kennelijk is de gedachte dat de Nederlandse toezichthouder wel bevoegd is binnen de Europese Unie maar niet daarbuiten. De bevoegdheid van de Nederlandse toezichthouder reikt echter niet verder dan de Nederlandse grens. Het wetsvoorstel brengt daarin geen verandering. Ook de verplichting om gegevens op te slaan binnen de Europese Unie kan dus onnodig belastend zijn voor aanbieders die wereldwijd actief zijn.

Conclusie

BCPA ziet niet goed hoe de strijdigheid met artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie en de belemmering van het vrij verkeer van diensten kan worden opgeheven, anders dan door intrekking van het wetsvoorstel. Een Nederlandse *alleingang* is zeer onwenselijk. Er zijn goede gronden voor de introductie van een vrijstelling van de verplichtingen uit hoofdstuk 13 Tw. voor 'kleine aanbieders'.

BCPA meent dat de eis om de betrokken gegevens binnen de Unie te bewaren en te verwerken onnodig is omdat deze niet bijdraagt aan een passend beschermingsniveau. Een passend beschermingsniveau kan nu reeds worden gewaarborgd in landen buiten de Europese Unie.

Ik vertrouw erop u met het bovenstaande voldoende te hebben geïnformeerd. Deze reactie bevat geen vertrouwelijke informatie.

Met vriendelijke groet,

secretaris BCPA

0 BD

30 januari 2015

Ministerie van Veiligheid en Justitie
?
Postbus 20301
2500 EA DEN HAAG

Uw kenmerk en datum:
Ons kenmerk

Geachte heer Mol-Lous,

Bij brief van 16 december 2014 heeft uw ministerie Vodafone Libertel B.V. tot 1 februari 2015 in de gelegenheid gesteld haar zienswijze te geven op het voorstel tot wijziging van de Telecommunicatie en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiedoeleinden. Bijgaand treft u onze zienswijze aan.

Aangezien de internetconsultatie formeel is gesloten is het voor Vodafone niet meer mogelijk om haar zienswijze via de website http:www.internetconsultatie.nl/dataretentie te uploaden.

Mocht u naar aanleiding van onze zienswijze nog vragen hebben dan kunt te allen tijde contact met mij opnemen.

Hoogachtend

Head of Regulatory Affairs & Digital Rights
judith.lichtenberg@vodafone.com

Vodafone Libertel B.V.
Simon Carmiggeltstraat 6,
1011 DJ Amsterdam

vodafone.nl

Reactie op de consultatie betreffende het voorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten ('Conceptwetsvoorstel')[1]

I Inleiding

1 Vodafone Libertel B.V. ('Vodafone') is ingevolge de Wet bewaarplicht telecommunicatiegegevens ('Wbt') verplicht om bepaalde telefonie- en internetgegevens te bewaren ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. De Wbt vormde destijds de implementatie van Richtlijn 2006/24/EG ('Dataretentierichtlijn').[2]

2 Op 8 april 2014 heeft het Hof van Justitie van de Europese Unie ('Hof van Justitie') de Dataretentierichtlijn met terugwerkende kracht ongeldig verklaard.[3] In reactie daarop heeft de regering op 18 november 2014 het Conceptwetsvoorstel in consultatie gegeven.

3 Het ministerie van Veiligheid & Justitie heeft Vodafone tot uiterlijk 1 februari 2015 in de gelegenheid gesteld haar zienswijze op het Conceptwetsvoorstel in te dienen.[4] Vodafone maakt hierbij graag en tijdig gebruik van deze mogelijkheid. Alvorens zij op het Conceptwetsvoorstel ingaat heeft zij eerst nog een aantal algemene opmerkingen.

II Algemene opmerkingen

4 Vertrouwen van klanten, andere eindgebruikers en investeerders in de sector (en de interneteconomie in zijn geheel) is essentieel voor onze bedrijfsvoering en ons business model. Onze klanten en gebruikers moeten er op kunnen vertrouwen dat hun communicatie vertrouwelijk blijft en dat hun persoonsgegevens bij ons in goede handen zijn. Zij hebben er recht op dat wij hun privacy respecteren en beschermen. Het recht op privacy van burgers is een fundamenteel recht, dat ook raakt aan de uitoefening van andere fundamentele rechten, zoals het recht op de vrijheid van meningsuiting.

5 Het recht op privacy is geen absoluut recht. Vodafone erkent het belang van de overheid om over adequate bevoegdheden en middelen te beschikken voor het bestrijden van ernstige misdrijven en bedreigingen van de staatsveiligheid en het beschermen van de fundamentele grondrechten en individuele vrijheden van elke burger, die essentieel zijn voor onze democratische rechtsstaat. Het rechtmatige gebruik van telecommunicatiegegevens voor opsporingsdoeleinden van de overheid kan aan de bescherming van fundamentele rechten en vrijheden bijdragen.

6 Ook hier geldt dat klanten, gebruikers en investeerders erop moeten kunnen vertrouwen dat het gebruik van telecommunicatiegegevens voor opsporingsdoeleinden door de overheid, inclusief de wijze waarop telecombedrijven invulling moeten geven aan hun wettelijke verplichtingen hieraan mee te werken, rechtmatig is en binnen de kaders van de democratische rechtsorde past. Dit betekent dat de overheid ervoor moet zorgen dat de inbreuk die daarbij wordt gemaakt op het

[1] Bijlage bij de brief van Minister Opstelten aan de Tweede Kamer d.d. 17 november 2014, Kamerstukken II 2014/14, 33 542, nr. 16.
[2] Richtlijn 2006/24/EG 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.
[3] HvJEU 8 april 2014, gevoegde zaken C-293/12 en C-594/12 (Digital Rights Ireland/Ireland en Seitlinger).
[4] Brief van het Ministerie van Veiligheid & Justitie aan Vodafone van 16 december 2014 met kenmerk 525682.

recht op privacy en andere fundamentele rechten, noodzakelijk is en tot een minimum wordt beperkt.

7 Vodafone stelt vast dat dit vertrouwen een deuk heeft opgelopen, onder andere door de ongeldigheidsverklaring van de Dataretentierichtlijn, dat ook vragen oproept over de geldigheid en proportionaliteit van de Wbt (zie hierna onderdeel III), de evaluatie van de Wbt[5] en de onthullingen van Edward Snowden over de praktijken van inlichtingendiensten als de NSA. Dit wordt onder meer bevestigd in het nieuwste rapport van de beveiligingsadviseur van de Europese Unie, ENISA.[6]

8 De combinatie van deze factoren heeft ook de behoefte aan betekenisvolle transparantie over het gebruik van telecommunicatiegegevens voor opsporingsdoeleinden doen toenemen.[7]

9 Om het vertrouwen in het gebruik van telecommunicatiegegevens voor opsporingsdoeleinden van de overheid en het draagvlak voor de rol van telecommunicatiebedrijven daarbij te herstellen en te behouden, is het volgens Vodafone cruciaal een helder wettelijk kader te scheppen dat up-to-date is en erin voorziet dat rekenschap wordt gegeven van nut, noodzaak, effectiviteit en proportionaliteit daarvan, op een wijze die kan worden getoetst en controleerbaar is.

10 Vodafone zal het bovenstaande hierna verder toelichten.

III De juridische status van de huidige Wbt

11 Het Hof van Justitie heeft de Dataretentierichtlijn in zijn geheel ongeldig verklaard wegens strijd met het Handvest van de grondrechten van de Europese Unie ('Handvest'). Volgens het Hof is het vereiste van proportionaliteit overschreden omdat de inmenging die de Dataretentie-richtlijn maakt op de artikelen 7 en 8 van het Handvest, onvoldoende nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke. Dit roept ook vragen op over de geldigheid en proportionaliteit van de Wbt.

12 Vodafone is zich ervan bewust dat het enkele feit dat de Dataretentierichtlijn ongeldig is verklaard niet betekent dat de Wbt ongeldig is. Volgens de Afdeling advisering van de Raad van State ('AARvS') is het Handvest tevens op de Wbt van toepassing maar is het 'in de eerste plaats de wetgever en uiteindelijk de Nederlandse rechter die het definitieve oordeel dient te geven over de vraag in hoeverre de Wbt in overeenstemming is met de artikelen 7 en 8 van het Handvest'.[8]

13 Aangezien de Wbt aan alle eisen voor de totstandkoming van Nederlandse formele wetgeving voldoet, is deze volgens het ministerie van Veiligheid & Justitie nog steeds geldig en dient deze zoals iedere wetgeving in beginsel te worden nageleefd.[9]

---

[5] De Wet bewaarplicht telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing, Wetenschappelijk onderzoek- en Documentatiecentrum, 2013 ('WODC-rapport').

[6] 'Privacy violations, revealed through media reports on surveillance practices have weakened the trust of users in the internet and e-services in general', in: ENISA Threat Landscape 2014, Overview of current and emerging cyber-threats, December 2014, p. iii www.enisa.europa.eu

[7] Zie bijvoorbeeld de vragen 121 en 122: *'Kan de minister in de toekomst transparantere en betekenisvollere gegevens over het aantal bevragingen publiceren?'* in Verslag van een schriftelijk overleg over evaluatie van de Wet bewaarplicht telecommunicatiegegevens, Kamerstukken 33870 Nr. 2.

[8] Advies van 17 juli 2014, bijlage bij de brief van Minister Opstelten aan de Tweede Kamer van 17 november 2014, Kamerstukken II 2014/14, 33 542, nr. 16, p.11 (Advies AARvS).

[9] Brief aan Vodafone van het ministerie van Veiligheid & Justitie van 18 december 2014.

14 De complicerende factor bij de naleving van de Wbt is volgens Vodafone echter dat de Wbt in haar huidige vorm, in de woorden van de AARvS naar verwachting 'het lot van de Dataretentierichtlijn zal delen, voor zover de Wbt materieel met de Dataretentierichtlijn overeenkomt'. Dit betreft volgens de AARvS o.a. 'de verplichting voor aanbieders van telecommunicatiediensten om bepaalde categorieën verkeers- en locatiegegevens te bewaren'.[10]

15 De AARvS heeft er daarnaast op gewezen dat de 'gevolgen van het arrest zich niet beperken tot het aanpassen of intrekken van de Wbt'. Volgens de AARvS zijn de EU-lidstaten gehouden om consequenties te trekken uit de ongeldigverklaring met terugwerkende kracht van de Dataretentie richtlijn. Dit kan meebrengen dat 'ook gevolgen van reeds uitgevoerde handelingen moeten worden teruggedraaid', waarbij kan worden gedacht aan de 'vernietiging van thans nog opgeslagen gegevens'.[11]

16 Bovendien is de Eerste Kamer van mening dat de regering er niet mee kan volstaan om de oude wet ongewijzigd te handhaven totdat het Conceptwetsvoorstel in werking is getreden.[12]

17 Hierdoor is bij klanten van Vodafone de perceptie ontstaan dat Vodafone thans uitvoering geeft aan een wet die een ongeoorloofde inmenging in de rechten van haar klanten oplevert. Klanten hebben hierover aan Vodafone hun zorgen geuit en concrete verzoeken ingediend om de verwerking van hun persoonsgegevens voor de uitvoering van de Wbt onmiddellijk te staken. Voor het noodzakelijke vertrouwen is het van belang dat de overheid alsnog zo spoedig mogelijk op een gemotiveerde en toegankelijke wijze uiteenzet op basis waarvan de Wbt in zijn huidige vorm dient te worden toegepast en de thans opgeslagen gegevens nog steeds moeten worden bewaard totdat het Conceptwetsvoorstel in werking is getreden.

IV Het Conceptwetsvoorstel

A. Eén wettelijk juridisch kader voor alle communicatiesurveillance

18 Deze consultatie richt zich uitsluitend op de aanpassing van de Wbt, terwijl de in paragraaf 9 genoemde uitgangspunten zouden moeten gelden voor alle surveillance activiteiten van communicatie. Dit zou er bijvoorbeeld toe moeten leiden dat ook verzoeken van de AIVD en de MIVD aan voorafgaande rechterlijke toetsing zijn onderworpen. Vodafone pleit er daarom voor dat alle wettelijke bevoegdheden in relatie tot communicatiesurveillance in onderlinge samenhang worden beoordeeld en in een helder, samenhangend wettelijk kader worden vervat, waarvan de legitimiteit onomstreden is . Daarbij is het van belang dat ook de operationele uitvoering door telecombedrijven en andere private partijen in de overwegingen worden meegenomen om te waarborgen dat de uitvoering door deze partijen op veilige, (kost) efficiënte wijze kan worden voldaan, waarbij de inbreuk op de privacy tot een minimum wordt beperkt.

19 Het Conceptwetsvoorstel bevat – conform het advies van de AARvS – een aantal beperkingen ten opzichte van de Wbt. Voor de legitimiteit van de aangepaste wetgeving is het cruciaal dat onomstreden is dat daarin aan alle bezwaren van het Hof van Justitie is voldaan.

[10] Advies AARvS, p. 11.
[11] Idem, p. 12.
[12] Brief van de Eerste Kamer aan de Minister van Veiligheid en Justitie van 10 december 2014 met kenmerk 145287.01.

B. Betekenisvolle transparantie

20 Op grond van de Dataretentierichtlijn was de overheid verplicht statistieken aan te leveren aan de Europese Commissie. Volgens de regering is dit 'gelet op de ongeldigverklaring van de richtlijn' niet meer 'aan de orde'.[13] Daarnaast is in de Telecommunicatiewet een regel opgenomen over de verplichting tot publicatie van het jaarlijks aantal bevragingen door opsporingsdiensten van gegevens over telecommunicatieverkeer.[14]

21 Sinds een aantal jaar publiceert de overheid jaarlijks 'indicatoren' ten aanzien van het aantal tapbevelen en het aantal bevragingen CIOT en dataretentie in het jaarverslag van het ministerie van Veiligheid & Justitie. Deze indicatoren geven echter onvoldoende inzicht in nut, noodzaak, effectiviteit en proportionaliteit van het gebruik van telecommunicatiegegevens voor opsporing.[15]

22 Vodafone is van mening dat het primair op de weg ligt van de overheid om rekenschap te geven van het gebruik van telecommunicatiegegevens voor opsporingsdoeleinden door hierover betekenisvolle informatie te verstrekken. Statistische gegevens over het aantal vorderingen vormen een onderdeel van deze informatie.[16]

23 Vodafone stelt voor om naast een verplichting voor de overheid tot publicatie van het jaarlijks aantal tapbevelen, bevragingen van CIOT en dataretentie, ook regels op te nemen over welke aanvullende informatie dient te worden gepubliceerd,[17] in welk format[18] en waaraan de gepubliceerde informatie dient te voldoen.[19] Uitgangspunt dient te zijn dat de informatie betekenisvol, toegankelijk en begrijpelijk is.

24 Daarnaast is het belangrijk dat de overheid uitlegt welke richtlijnen en procedures van toepassing zijn om de uitoefening van opsporingsbevoegdheden met waarborgen te omkleden en inzichtelijk te maken in welke mate deze waarborgen in de praktijk worden gevolgd. Dit laatste kan bijvoorbeeld door rapporten (of samenvattingen daarvan) waarin verslag wordt gedaan van

---

[13] Zie antwoorden 72 en 73 in Verslag van een schriftelijk overleg over evaluatie van de Wet bewaarplicht telecommunicatiegegevens, Kamerstukken 33870 Nr. 2.

[14] Artikel 13.4 lid 4 Tw juncto artikel 8 Besluit verstrekking gegevens telecommunicatie.

[15] Het WODC merkt hierover o.a. op: "*Deze cijfers geven bijvoorbeeld geen inzicht in de mate waarin Nederlandse opsporingsdiensten een inbreuk maken op de privacy van verdachten en betrokkenen door de inzet van deze middelen of in het aantal personen van wie er jaarlijks telecommunicatiegegevens worden opgevraagd, of van het aantal opsporingsonderzoeken of de aard van de opsporingsonderzoeken waarvoor deze gegevens worden opgevraagd. Ook geven de cijfers geen inzicht in de mate waarin een vordering daadwerkelijk tot een verstrekking van de gegevens heeft geleid*", WODC rapport. Zie ook noot 7.

[16] Vodafone geeft er de voorkeur aan dat statistische gegevens van alle vorderingen en bevelen die in een bepaalde periode in Nederland zijn gedaan, centraal door de overheid worden gepubliceerd om twee redenen: (1) Geen enkele individuele operator kan een volledig beeld schetsen, noch heeft een operator inzicht in de context van een onderzoek. Het is belangrijk om de verzoeken aan alle operators in kaart te brengen en 2) Operators hanteren verschillende werkwijzen als het gaat om vastleggen en rapporteren van dezelfde statistische informatie.

[18] In het WODC rapport wordt bijvoorbeeld gesuggereerd om de uitgave van het Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime als leidraad te gebruiken, WODC rapport, p 124 en voetnoot 116.

[19] Vodafone meent dat de statistieken in ieder geval aan de volgende criteria dienen te voldoen: a) onafhankelijk getoetst, bediscussieerd en geverifieerd vóór publicatie, b) uitleg bevatten welke methode is gebruikt bij het opslaan en analyseren van de geaggregeerde aantallen verzoeken die zijn gepubliceerd, c) alle categorieën verzoeken omvatten, of indien dit niet het geval is, vermelden welke categorieën niet zijn opgenomen, voorzien van een uitleg waarom zij niet worden vermeld, d) alle verzoeken omvatten die in Nederland in een bepaalde periode zijn gedaan.

periodieke audits en evaluaties van de wettelijke bevoegdheden van de overheid en de wijze waarop aan deze bevoegdheden uitoefening wordt gegeven, standaard te publiceren.

C. Noodzaak van de bewaarplicht

25 In de memorie van toelichting constateert de regering terecht dat de situatie van nu anders is dan de situatie van voor 2009. Uit de evaluatie van de Wbt volgt onder meer dat de Wbt als gevolg van de snelle technologische ontwikkelingen en de digitalisering van de samenleving is verouderd, gegevens van burgers worden bewaard die niet of nauwelijks door opsporingsdiensten worden gebruikt en dat de effecten tot harmonisatie van de bewaartermijnen nauwelijks zijn te meten en te onderscheiden.[20] Een ander gevolg van de digitalisering van de samenleving is dat de inbreuk die de opsporingsbevoegdheden maken op de privacy van burgers significant is vergroot.[21]

26 Voor nut, noodzaak en efficiëntie van het gebruik van telecommunicatiegegevens voor opsporingsdoeleinden is het een vereiste dat de toepasselijke wetgeving up-to-date is. In de memorie van toelichting wordt opgemerkt dat het in 2009 voor aanbieders noodzakelijk was om voor bedrijfsdoeleinden verkeersgegevens en internetgegevens te bewaren maar dat 'is nu bij veel contracten als gevolg van technologische ontwikkelingen niet meer noodzakelijk'. Vodafone begrijpt niet wat hiermee wordt bedoeld.

D. Bedrijfseffecten

27 De regering merkt terecht op dat het Conceptwetsvoorstel tevens gevolgen zal kunnen hebben voor de bedrijfsvoering van de in Nederland opererende internet- en telecomaanbieders. Vodafone wijst er op dat naast de in de memorie van toelichting genoemde verplichting tot opslag van gegevens op het grondgebied van de Europese Unie ook andere wijzigingen in het Conceptwetsvoorstel consequenties kunnen hebben voor de bedrijfsvoering en de kosten van de aanbieders. Hierbij kan worden gedacht aan het voorstel om de formulering van IP adressen aan te passen. Vodafone stelt het op prijs dat de precieze bedrijfseffecten en kosten in samenwerking met het bedrijfsleven in kaart zullen worden gebracht en zij zal hieraan haar volledige medewerking verlenen. Vodafone meent dat het uitgangspunt moet zijn dat eventuele (investerings)kosten van telecomaanbieders volledig worden vergoed.

E. Toezichthouders

28 Vodafone is voorstander van toezicht door toezichthouders op haar bedrijfsprocessen om uitvoering te geven aan haar medewerkingsplichten. Nu de eigen bevoegdheden van Vodafone om hierover transparant zijn, aanzienlijk worden beperkt door geheimhoudingsverplichtingen, is dit een manier waardoor Vodafone alsnog rekenschap kan afleggen dat zij haar processen in de praktijk met waarborgen omkleedt. Vodafone begrijpt echter niet goed waarom de privacy wordt vergroot als de toezichthouders ook de bevoegdheid krijgen om gegevens feitelijk in te zien.

V. Conclusie

29 Om het noodzakelijke vertrouwen in het gebruik van telecommunicatiegegevens en andere vormen van communicatie surveillance activiteiten voor opsporingsdoeleinden door de overheid en de rol van private partijen daarbij te herstellen en te behouden is het cruciaal dat een helder, samenhangend wettelijke kader wordt geschapen, inclusief het Conceptwetsvoorstel, dat up-to-

[20] WODC rapport, p. 20.
[21] WODC rapport, voorwoord en p. 35-36.

date is en rekenschap geeft van nut, noodzaak, effectiviteit en proportionaliteit daarvan, op een wijze die kan worden getoetst en controleerbaar is. Dit betekent dat het Conceptwetsvoorstel voldoende tegemoet moet komen aan de bezwaren van het Hof van Justitie, waarbij tevens rekening wordt gehouden met operationele uitvoeringseisen en een duidelijke transparantieverplichting voor de overheid bevat, zodat de legitimiteit van het Conceptwetsvoorstel onomstreden is.

NEDERLANDSE
VERENIGING
VOOR RECHTSPRAAK

De Minister van Veiligheid en Justitie
Mr. I.W. Opstelten
Postbus 20301
2500 EH DEN HAAG

Datum
17 februari 2015

Uw kenmerk

Contactpersoon

Onderwerp
Advies op het conceptwetsvoorstel inzake de 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

Geachte heer Opstelten,

Bij brief van 18 november 2014 heeft u de Nederlandse Vereniging voor Rechtspraak (hierna: NVvR) om advies gevraagd over het conceptwetsvoorstel inzake de 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 Dit advies is voorbereid door de leden van de vereniging en vastgesteld door de Wetenschappelijke Commissie van de NVvR.

Strekking wetsvoorstel

Het wetsvoorstel voorziet in de aanpassing van de Telecommunicatiewet en betreft 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. Daarbij worden de verschillende categorieën van te bewaren gegevens beperkt tot de gegevens die stikt noodzakelijk zijn voor de opsporing en vervolging van ernstige misdrijven. Voorts wordt voorgeschreven dat de telecommunicatiegegevens op het grondgebied van de Unie worden bewaard. Het 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 aangepast, zodat de bewaarde gegevens slechts gedurende een periode van zes maanden kunnen worden geraadpleegd ten behoeve van de opsporing of vervolging van strafbare feiten waarvoor voorlopige hechtenis mogelijk is.

NVvR • Postbus 30315 • 2500 GH Den Haag
088-3611300 • info@nvvr.org • www.nvvr.org

Advies

Algemeen

Het Europese Hof van Justitie heeft in zijn uitspraken van 8 april 2014 in de zaken C-293/12 en C-594/12 de Europese dataretentie richtlijn (2006/24/EG) ongeldig verklaard. De uitspraken hebben de wetgever genoopt tot een kritische blik naar de huidige regeling van dataretentie en vormen een directe aanleiding voor het thans voorliggende wetsvoorstel. De NVvR onderschrijft dat de wet in het belang van het recht op privacy van de burger de nodige waarborgen dient te bieden ter bescherming en beveiliging van diens bewaarde telecommunicatiegegevens, temeer waar het gaat om de toegang tot de gegevens, de technische beveiliging van de bewaaromgeving en de opslag binnen de Europese Unie. Anderzijds wijst de NVvR erop dat de wet zó moet zijn ingericht dat de veiligheid van de burger evenzeer optimaal kan worden beschermd door het politiële en justitiële apparaat en dat daarbij moet worden onderkend dat telecommunicatiegegevens (gebruikers- en verkeersgegevens) in de praktijk van groot belang blijken te zijn voor een effectieve opsporing en vervolging.[1] Het recht van de burger op veiligheid is immers evenzeer een groot goed, net als diens recht op privacy. Hiertussen moet worden gezocht naar een balans, hetgeen ook in de genoemde uitspraken van het Europese Hof van Justitie tot uitdrukking wordt gebracht.

De vraag kan worden gesteld of die balans met het voorliggende wetsvoorstel – met name waar het gaat om (de verkorting van de termijn van) de bewaarplicht – niet onevenredig is doorgeslagen ten gunste van het recht op privacy. Tevens kan de vraag worden gesteld of dit niet ten koste gaat van de opsporingspraktijk van de officier van justitie en daarmee de veiligheid van de burger. Tenslotte vraagt de NVvR zich af of het wetsvoorstel niet méér bescherming beoogt te bieden dan het Europese Hof blijkens de hierboven genoemde uitspraken van de Lidstaten verlangt. De NVvR vreest dat het strafrechtelijk systeem verder onder druk zal komen te staan doordat het wetsvoorstel een wijziging beoogt in de toetsende autoriteit, hetgeen een groei aan administratieve lasten met zich mee zal brengen, terwijl juist één van de doelstellingen van de op handen zijnde hervorming van het wetboek van strafvordering is om de administratieve belasting van de strafrechtsketen terug te brengen. Ook meent de NVvR dat de wijziging van de toetsende autoriteit tevens een wettelijke systeembreuk betekent, hetgeen hieronder verder uiteen zal worden gezet, waarbij bovendien moet worden opgemerkt dat de uitspraken van het Europese Hof in de visie van de NVvR ook op dit punt niet tot een dergelijke wijziging nopen.

Inhoudelijk

Opgemerkt zij vooreerst dat gebruikers- en verkeersgegevens geen informatie bevatten over de *inhoud* van de communicatie. Indien men van de inhoud van telefonie- en internetcommunicatie wil kennisnemen, is dat alleen mogelijk door middel van interceptie. Hiervoor is een machtiging van de rechter-commissaris nodig. Voor het beschikbaar maken van de gebruikers- en verkeersgegevens voor opsporingsdiensten, is een gerichte vordering van de officier van justitie aan de aanbieder nodig. Bij het doen van die vordering toetst de

[1] "De Wet bewaarplicht Telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing." ISBN 978-94-6236-041-9.

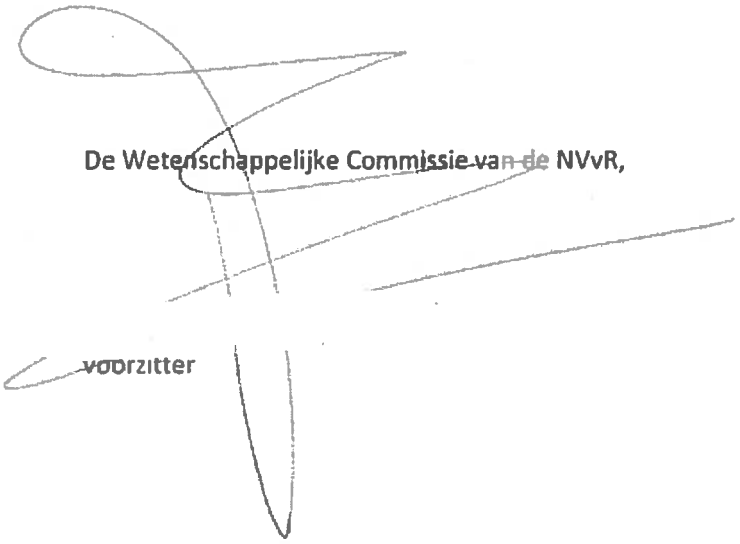
officier van justitie aan de beginselen van proportionaliteit en subsidiariteit, zodat alleen die gegevens worden verkregen die strikt noodzakelijk zijn voor het opsporen van strafbare feiten. Het gebruik van de gegevens wordt ten slotte beoordeeld door de zittingsrechter indien het tot een strafzaak komt. In de praktijk zijn geen gevallen bekend waarin de toepassing van de huidige regeling door de rechter als onrechtmatig is aangemerkt.
Het bewaren en gebruiken van verkeersgegevens voor de opsporingspraktijk houden derhalve een beperkte inbreuk op de privacy van de gebruiker in, terwijl de huidige regeling met de nodige waarborgen is omkleed.

Beperking periode bewaarplicht
De bewaarplicht van gebruikers- en verkeersgegevens ten behoeve van de opsporing van strafbare feiten is, zoals ook het Europese Hof constateert, als zodanig niet strijd met het recht van de Europese Unie c.q. de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie of artikel 8 van het EVRM. Artikel 7 en 8 van het Handvest en artikel 8 EVRM vereisen dat de bewaartermijn een 'beperkte periode' betreft. De NVvR vindt in de bovengenoemde uitspraken noch in het Europese recht aanknopingspunten voor de veronderstelling dat de huidige wettelijke bewaartermijnen van 12 maanden voor telefoniegegevens en 6 maanden voor internetgegevens niet zou kunnen worden aangemerkt als een dergelijke 'beperkte periode' en dat een wetswijziging op dit punt noodzakelijk zou zijn.
Bovendien voorziet de NVvR dat in de praktijk als gevolg van een dergelijke beperking van de periode van bewaarplicht beduidend minder strafbare feiten zullen kunnen worden opgespoord en opgelost dan thans het geval is.
Gelet op het belang van de telecommunicatiegegevens voor de opsporings- en vervolgingspraktijk bij het handhaven van de huidige bewaartermijn - overigens ook hier afgewogen tegen de relatief beperkte inbreuk op het privacy-recht -, adviseert de NVvR met klem om een algemene verplichting tot het bewaren van telecommunicatiegegevens voor de duur van de huidige wettelijke termijn in stand te laten en deze niet verder te beperken.

Toegang tot de bewaarde gegevens
Het wetsvoorstel maakt voor wat betreft de toegang tot de bewaarde gegevens onderscheid 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 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. 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. De voorgestelde wijziging komt gedifferentieerd neer op een halvering van de huidige bewaartermijnen. Beoogd wordt om hiermee aan de hand van een objectief criterium nadere differentiatie aan te brengen in de beschikbaarstelling van de gegevens. Een dergelijk differentiatie zoals die thans concreet wordt voorgesteld, komt de NVvR onwenselijk voor.
De praktijk is vaak weerbarstig, en de feiten gecompliceerder. In de praktijk zal bij de aanvang van een opsporingsonderzoek niet altijd aanstonds duidelijk zijn hoe de uiteindelijke kwalificatie van de feiten waar het opsporingsonderzoek zich op richt, zal luiden, en zal gaande het opsporingsonderzoek kunnen blijken dat de feiten ernstiger,

structureler of meer georganiseerd zijn dan deze zich aanvankelijk lieten aanzien. De bevoegdheden 'opschalen' zal bij een regeling als thans is voorgesteld, mogelijk geen zin meer hebben omdat de termijn voor bevraging van gegevens inmiddels verstreken zal zijn. De relatief korte bewaartermijnen zullen bij dergelijke ontwikkelingen in een opsporingsonderzoek fataal kunnen blijken te zijn. Bij dit alles verdient aandacht dat er ernstige strafbare feiten zijn aan te wijzen met een grote maatschappelijke impact waarvan de maximale strafdreiging lager is dan zes jaar. Gedacht kan worden aan delicten als gewoonteheling, seriematige ladingdiefstallen, ramkraken, gewoontewitwassen. In dergelijke onderzoeken zou de opsporing bemoeilijkt worden door de thans voorgestelde verkorte termijn van zes maanden.
De NVvR adviseert de Minister om af te zien van de voorgestelde regeling.

Toetsingsautoriteit
In het wetsvoorstel wordt de rechter-commissaris geïntroduceerd als de toetsende autoriteit. De rechter-commissaris zou dan in plaats komen van de officier van justitie die daartoe in de huidige regeling bevoegd is. De memorie van toelichting gaat echter niet in op de achtergrond van deze wijziging. Weliswaar overwoog het Hof van Justitie – zoals ook opgenomen in de memorie van toelichting - dat de gewraakte Europese 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, en dat de toegang van de bevoegde autoriteiten tot de bewaarde gegevens niet afhankelijk was gesteld van voorafgaande toetsing door een gerecht of een onafhankelijk bestuurlijk orgaan naar aanleiding van een gemotiveerd verzoek van de aangewezen autoriteiten, doch de NVvR merkt op dat in haar visie uit de uitspraken van het Hof van Justitie niet (zonder meer) volgt dat de officier van justitie als toetsende autoriteit binnen het huidige wettelijk kader niet zou voldoen. De officier van justitie moet bovendien – ook naar Europese maatstaven - heel wel in staat worden geacht en in een voldoende onafhankelijk positie verkeren om in concrete strafzaken een dergelijke toets aan het proportionaliteit- en subsidiariteitsbeginsel te kunnen doen.
Bovendien koerst deze wijziging aan op een systeembreuk. Het wetboek van strafvordering gaat thans uit van de gedachte dat hoe zwaarder de inbreuk is op de privacy, hoe 'hoger' de toetsende autoriteit. Vanuit die gedachte alsmede gelet op de regelingen die ingrijpendere bijzondere bevoegdheden tot opsporing op bevel van de officier van justitie bevatten, vermag de NVvR niet in te zien waarom een minder ingrijpende bevoegdheid tot het vorderen van gebruikers-/verkeersgegevens, waar hier sprake van is, de officier van justitie zou moeten worden ontnomen en aan de rechter-commissaris zou moeten worden toegekend.
Daarnaast voorziet de NVvR dat de voorgestelde regeling onmiskenbaar zal leiden tot een grote toename van het aantal vorderingen die bij de rechter-commissaris zullen worden ingediend. Vertragingen in de gang van zaken binnen het kabinet van de rechter-commissaris zullen onvermijdelijk zijn bij een gelijkblijvende bezetting, met alle onwenselijke gevolgen van dien voor tal van procedures waarin de rechter-commissaris een rol heeft.
De NVvR verzoekt de Minister dan ook af te zien van deze wijziging in toetsingsautoriteit in het wetsvoorstel.



De Wetenschappelijke Commissie van de NVvR,

voorzitter

Voorontwerp van wet tot wijziging van de Telecommunicatiewet en het WvS in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten

Reactie van KPN

KPN
Postbus 30 000
2500 GA Den Haag
Kenmerk: GCO/15/U/004

30 januari 2015

Inleiding

Bij brief van 16 december 2014 is namens de Minister van Veiligheid en Justitie aan "Marktpartijen vertegenwoordigd in het P 13 samenwerkingsverband" gevraagd om een reactie op het concept-wetsvoorstel tot aanpassing van de wettelijke regeling van de bewaarplicht, uiterlijk op 1 februari 2015. KPN voldoet graag aan dat verzoek, mede omdat in de publieke discussie over de bewaarplicht de rol van aanbieders daarin vaak aan de orde wordt gesteld. In dit document is de reactie van KPN neergelegd.

Achtergrond van het wetsvoorstel

Op 8 april 2014 heeft het Europese Hof van Justitie van de Europese Unie U de zogenaamde Dataretentierichtlijn (2006/24/EG) ongeldig verklaard. De Richtlijn bevatte regels gericht tot de lidstaten met betrekking tot aanpassing van de wetgeving over dataretentie in verband met de bestrijding van zware misdaad. Het HvJ EU heeft geoordeeld dat de Richtlijn in strijd is met Europees recht omdat (kortweg):

- er teveel gegevens worden opgeslagen van teveel personen;
- onvoldoende is geregeld wie onder welke omstandigheden toegang kan krijgen tot de bewaarde gegevens;
- niet is gewaarborgd dat gegevens niet langer worden bewaard dan strikt noodzakelijk;
- niet is gewaarborgd dat de bewaarde gegevens voldoende zijn beveiligd tegen misbruik en onrechtmatige toegang.

Nog op de dag van de uitspraak is namens marktpartijen al aan de overheid verzocht om zo snel mogelijk duidelijkheid te verstrekken over de gevolgen van deze uitspraak voor de Nederlandse wet en uitvoeringspraktijk.[1] Over die gevolgen van de ongeldigverklaring van de richtlijn voor de Nederlandse Wet bewaarplicht heeft de Raad van State desgevraagd al in juli advies uitgebracht.[2] Hoewel de Raad constateert dat de Nederlandse wetgeving niet direct door de onverbindendverklaring van de richtlijn waarop zij was gebaseerd wordt geraakt, overweegt hij dat de wettelijke regeling van de bewaarplicht zoals die thans in de wet is neergelegd strijdig is met Europese recht en dat de wet dus moet worden aangepast, in het bijzonder de artikelen 7 en 8 van het Handvest van de grondrechten van de EU.

In zijn brief aan de Tweede Kamer van 17 november 2014[3] onderschrijft de Minister van V&J deze conclusie. Ook pas op dat moment werd het advies van de Raad van State openbaar. Bij die brief presenteerde de Minister ook het wetsvoorstel waarop thans reactie wordt gevraagd.

Deze situatie roept (ten minste) twee vragen op:

- Hoe dient de wet te worden aangepast om te voldoen aan de Europese regels? In wezen is dat de vraag om de beoordeling van het voorliggende wetsvoorstel waar de Minister de reactie van marktpartijen om vraagt.
- Wat betekent de conclusie dat de huidige wet in strijd is met de Europese regels tot het moment dat de wet daarop is aangepast voor de praktijk? Die vraag wordt – volgens KPN – tot dit moment door de Minister teveel genegeerd. In deze reactie zal KPN daarom ook op dat punt ingaan.

---

1 http://www.nederlandict.nl/?id=13350.

2 Zie *Srcrt*. 2015, 328.

3 *Kamerstukken II* 2014/15, 33 542, nr. 16, p. 7-8.

Noodzaak en uitvoering van een bewaarplicht

Een belangrijk element bij de beoordeling van het wetsvoorstel is de vraag of een algemene bewaarplicht proportioneel en passend kan zijn in het licht van het daarmee te bereiken doel. Zoals het HvJ EU aangeeft gaat het om een zeer vergaande inbreuk op de met de artikelen 7 en 8 van het Handvest beschermde grondrechten. Volgens KPN is het van cruciaal belang dat de Minister zeer nauwkeurig en diepgaand motiveert wat de noodzaak van de bewaarplicht is in het licht van de daarmee nagestreefde belangen en dat de invulling van die plicht niet verder gaat dan strikt noodzakelijk is.[4] In zijn hoedanigheid van aanbieder van telecomdiensten is KPN onderworpen aan de verplichting tot bewaring en verstrekking van de in de wet benoemde gegevens. KPN wordt daarmee betrokkene in de afweging van de belangen van haar klanten op privacy en vrijheid van communicatie tegenover de belangen van (staats-)veiligheid en bestrijding van ernstige criminaliteit, zonder dat zij evenwel in staat is zich inhoudelijk een oordeel over nut en noodzaak van die inbreuk te geven. Terecht vernemen aanbieders immers op geen enkele manier waarvoor de bewaarde en gevraagde gegevens noodzakelijk zijn en is aan hen een grote mate van beveiliging en geheimhouding opgelegd. Maar juist die conclusie – dat aanbieders betrokkene zijn, maar zonder mogelijkheid van beoordeling en controle – betekent eens te meer dat het de overheid is die de maximale openheid moet geven die, met inachtneming van de betrokken belangen, mogelijk is.

In dit opzicht merkt KPN dat de overheid vaak een zeer restrictieve invulling geeft aan de bewijslast en openheid, die juist noodzakelijk zou zijn om vertrouwen te geven dat de verplichtingen noodzakelijk zijn en correct en proportioneel worden ingevuld. Volgens KPN is het de rol van de politiek om deze belangen af te wegen en daarop de controle te houden. Aanbieders worden verplicht tot naleving van tegenstrijdige normen (privacy- en communicatiebescherming vs. medewerking aan inbreuken daarop door de overheid), maar zij kunnen in die afweging geen inhoudelijke betrokkenheid hebben. Dat vergt dan ook extra aandacht bij de behandeling van het wetsvoorstel en de (controle op de) naleving daarvan. In ons democratisch rechtsbestel is het de taak van het parlement hierin afwegingen voor de wetgeving te maken en de uitvoering door de overheid te controleren. KPN kan daarin in haar hoedanigheid van 'aanbieder' geen andere rol hebben dan andere ondernemingen.

Voorafgaand aan de HvJ EU uitspraak heeft de Minister het WODC een evaluatie laten uitvoeren met betrekking tot de huidige wettelijke regeling.[5] Hoewel ook in dat onderzoek weinig kwantitatieve informatie is te vinden naar noodzaak en proportionaliteit van de bewaarplicht komt daaruit wel naar voren dat de ontwikkeling van de communicatiemarkt grote invloed daarop heeft. Steeds meer communicatie vindt plaats over internet, maar valt daarmee vaak ook buiten de gegevens waarop de bewaarplicht ziet. Van de bewaarde gegevens van internet wordt zeer weinig gebruik gemaakt. Die ontwikkeling duidt dus op een afnemende effectiviteit van de bewaarplicht en dat zou bij de beoordeling een rol moeten spelen. Naar aanleiding van de evaluatie gaf de Minister in zijn aanbiedingsbrief aan de Tweede kamer nog aan dat hij de evaluatie zou gebruiken om te onderzoeken 'de lijst met te bewaren gegevens (...) uit te breiden'. Maar terecht blijkt uit het voorontwerp dat thans niet meer alleen naar wensen en uitbreiding van te bewaren gegevens wordt gekeken, maar veel meer naar noodzaak en proportionaliteit. De uitspraak van het HvJ EU laat ook geen nadere benadering toe.

Voorgestelde aanpassingen in de bewaarplicht

Het wetsvoorstel komt inhoudelijk in het kort hierop neer:

---

[4] Een eenvoudige rekensom leert dat het aantal gerapporteerde bevragingen afgezet tegen het aantal door ACM uitgegeven vaste en mobile telefoonnummers meebrengt dat 99,998 % van alle data wordt bewaard zonder dat om deze informatie wordt gevraagd.

[5] 'De Wet bewaarplicht telecommunicatiegegevens', WODC rapport 310, 2013, Bijlage bij brief van de Minister van 12 februari 2014, *Kamerstukken II* 2013/14, 33 870, nr.1.

- De eisen ten aanzien van de beveiliging van de bewaarde gegevens kunnen worden verzwaard.
- De gevallen waarin toegang tot de gegevens kan worden verkregen worden beperkt. Gegevens ouder dan zes maanden zullen uitsluitend nog kunnen worden opgevraagd bij aangewezen categorieën ernstige misdrijven en als aan aangescherpte procedurele vereisten (toestemming van de R-C) is voldaan.
- Gegevens mogen uitsluitend binnen de Europese Unie worden bewaard.
- De bewaartermijn blijft gelijk.
- De te bewaren gegevens blijven grotendeels gelijk, met dien verstande dat:
    - de bewaarplicht voor MMS/EMS komt te vervallen;
    - de afzonderlijke bewaarplicht zoals die nu geldt voor internettelefonie komt te vervallen. De bewaarplicht voor internettelefonie wordt gelijkgetrokken met de bewaarplicht voor gewone telefonie (zoals in de praktijk al werd geïnterpreteerd);
    - de afzonderlijke bewaarplicht voor e-mail komt te vervallen;
    - bij internetgegevens zal de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie niet langer bewaard worden;
    - bij internetgegevens dient het opgeslagen IP-adres zodanig te zijn dat de gebruiker is te identificeren. Indien dat in de infrastructuur niet zodanig is voorzien zijn aanvullende maatregelen vereist. Naast het IP-adres zoals dat nu bewaard moet worden, moeten de daaraan gerelateerde poortnummers worden opgeslagen nodig om de gebruiker te identificeren.

Een betere bescherming van de betrokken grondrechten?

De beoordeling van het voorstel zal moeten inhouden dat wordt bezien of met deze aanpassingen wel aan de door het HvJ EU gestelde eisen wordt voldaan. Vastgesteld moet worden dat de aanpassingen in (i) de gevallen waarin de gegevens door bevoegde instanties mogen worden gevraagd en (ii) de procedure die aan verstrekking vooraf gaat, wel invloed hebben op het (mogelijk verminderde) gebruik van de gegevens, maar niet op de bewaring als zodanig. Grotendeels dienen dezelfde gegevens bewaard te worden, hooguit zal eventueel aan aanvullende eisen ten aanzien van beveiliging moeten worden voldaan.

Aan het principiële bezwaar dat de bewaring als zodanig al een inbreuk is op de betrokken grondrechten wordt met de aanpassing niet verder tegemoet gekomen. Of de belangenafweging daarmee thans wel op voldoende wijze heeft plaatsgevonden valt op basis van publieke informatie moeilijk te beoordelen. Hier ligt het grootste probleem bij de beoordeling van het wetsvoorstel. KPN beseft dat een deel van de informatie die noodzaak en proportionaliteit van de bewaarplicht moet onderbouwen vertrouwelijk moet blijven in het kader van (staats-)veiligheid en criminaliteitsbestrijding. Maar het zou bij de totstandkoming van de wet wel noodzakelijk zijn dat wordt gezocht naar manieren om die informatie te kunnen delen met het parlement (en voordien de Raad van State), teneinde wel de noodzakelijke controle van de abstract gebruikte argumenten te kunnen wegen. Dit geldt vooral ook de noodzaak om de bewaarplicht qua termijnen in stand te laten.

Ten aanzien van de (procedurele) aanpassingen die leiden tot beperking van de gevallen waarin de gegevens mogen worden opgevraagd en gebruikt is er wel een verdergaande aanpassing bescherming bereikt. In elk geval betekenen deze wijzigingen voor KPN een verbeterde waarborg tegen te lichtvaardig gebruik van de gegevens.

Gevolgen van de aanpassingen voor betrokken aanbieders

Voor de betrokken ondernemingen zullen vooral de mogelijke aanpassingen van beveiligingseisen en de aanpassingen ten aanzien van de mogelijkheid om IP adressen aan gebruikers te relateren praktische – en misschien zelfs aanzienlijke – gevolgen (kunnen) hebben. Deze punten raken aan de principiële vraag in hoeverre de kosten voor noodzakelijke aanpassingen redelijkerwijs nog op de aanbieders kunnen worden afgewenteld.

De bewaring van de betrokken gegevens gedurende de in de wet opgedragen termijnen is voor een belangrijk deel van de gegevens geen activiteit die past binnen de bedrijfsvoering van de betrokken aanbieders. Zij dienden bij de invoering van de bewaarplicht een – in elk geval voor KPN – omvangrijk en kostbaar project uit te voeren om te voldoen aan de toen bij wet opgelegde verplichtingen. Zoals uit het WODC rapport al blijkt staat wel vast dat een deel van de activiteiten die daarbij moesten worden verricht feitelijk nutteloos zijn geweest, omdat de benoemde gegevens – vooral ten aanzien van 'internet' – geen daadwerkelijk nut hadden en in de praktijk ook zelden of nooit zijn gevraagd. Ook betekende de wettelijke regeling een verzwaring in die zin dat bij alle nieuwe dienstintroducties en systeemaanpassingen een veel grotere complexiteit is ontstaan dan voor de bedrijfsvoering nodig zou zijn. Thans geeft de Minister toe dat een deel van deze gegevens niet nodig zijn. Door de manier waarop de lijst van te bewaren gegevens tot stand is gekomen (meer op basis van indrukken van wenselijkheid dan op basis van werkelijke beoordeling van noodzaak en proportionaliteit) hebben aanbieders dan ook veel onnodige kosten moeten maken en onnodige complexe bedrijfsprocessen moeten inrichten.

Dit alles illustreert dat de wettelijke regeling, waarin aanbieders niet worden gecompenseerd voor inrichting en aanpassing van systemen teneinde aan de wet te voldoen, geen prikkel geeft aan de overheid om tevoren reeds afwegingen te maken naar nut en noodzaak van die aanpassingen. Alleen dat al zou tot heroverweging van de financieringsmethodiek moeten leiden. In dit opzicht strekt het Verenigd Koninkrijk tot voorbeeld, waarin de overheid met aanbieders afspraken maakt over de noodzakelijke aanpassingen, maar daarvoor die aanbieders dan ook vergoedt.

Ten aanzien van de in het wetsvoorstel opengelaten optie om voorschriften ten aanzien van beveiliging van de gegevens te verzwaren merkt KPN op dat het zeer onbevredigend is dat thans haar reactie wordt gevraagd op voorstellen waarvan de omvang nog volstrekt onzeker is. Op zich meent KPN al aan strenge eisen van beveiliging van de gegevens te voldoen, maar niet uit te sluiten valt dat er met de technologische mogelijkheden steeds verbeterde methoden van beveiliging komen. Het zou echter onwenselijk en disproportioneel zijn om de door de overheid 'uitbestede bewaarplicht' zo in te vullen dat daar met regelmaat op eigen kosten weer nieuwe investeringen in gedaan zouden moeten worden.

Ten aanzien van de nieuw voorgestelde eis dat aanbieders steeds de mogelijkheid moeten hebben om eindgebruikers aan (externe) IP-adressen te relateren constateert KPN dat dit kan leiden tot complexe, tijdrovende en kostbare aanpassingen van systemen. De dienstverlening rondom internet ontwikkelt zich snel en de wensen van gebruikers al evenzeer. Het is thans niet te voorspellen in hoeverre een dergelijke 'resultaatsverplichting' in de toekomst redelijkerwijs na te leven zal zijn. De technologische ontwikkelingen van internet zijn niet gebaseerd op Nederlandse wettelijke eisen in het kader van een bewaarplicht. 'Juist niet', zouden sommige voorvechters van een vrij en open internet bepleiten! Met deze formulering wordt op een zeer technologie-afhankelijke wijze een verplichting opgelegd waarvan de praktische omvang niet voorzien kan worden. KPN acht deze aanpassing dan ook niet proportioneel. Zeker omdat de kans bestaat dat de technologische ontwikkelingen kunnen meebrengen dat deze eis niet op de beschreven wijze zal zijn in te vullen, zou het ook hier beter zijn te kiezen voor een systeem waarbij een doel wordt beschreven dat in overleg tussen aanbieders en behoeftestellers – en op kosten van deze laatste – kan worden ingevuld. Indien al een aanpassing op dit gebied wordt overwogen zal een adequate implementatietijd moeten worden toegepast. De noodzakelijke lengte daarvan zal afhangen van de concrete ver-

plichting die uiteindelijk zal worden opgenomen, maar duidelijk is wel dat bij de huidige formulering een implementatietermijn van minimaal een jaar al kort zou zijn.

KPN kan zich er in vinden dat het wetsvoorstel geen onnodige uitbreiding van de bewaarplicht inhoudt ten aanzien van locatiegegevens (zoals de 'last cell ID'; MvT, p. 20). Het zou geheel tegen de uitspraak van het HvJ EU ingaan om de toch al te ruime kring van te bewaren gegevens nog uit te breiden zonder absolute noodzaak.

Gevolgen van overgangsperiode

In de al eerder genoemde brief van de Minister van V&J van 17 november 2014 aan de Voorzitter van de Tweede Kamer[6] staat: *'De Afdeling advisering stelt vast dat de Wet bewaarplicht telecommunicatiegegevens de door het Hof van Justitie gewraakte bepalingen van de richtlijn dataretentie omzet en dat toetsing van de Wet bewaarplicht telecommunicatiegegevens aan het Handvest van de grondrechten tot de conclusie leidt dat deze wet, net als de richtlijn dataretentie, in strijd is met de artikelen 7 en 8 van het Handvest van de grondrechten. Hieruit vloeit voort dat de nationale wetgeving moet worden aangepast voor zover deze niet in overeenstemming is met het Handvest van de grondrechten. De Nederlandse regering kan deze zienswijze onderschrijven.'* (onderstreping toegevoegd).

De beide onderstreepte passages geven echter niet alleen aan dat er noodzaak is de wet aan te passen, maar impliciet ook dat uitvoering van de huidige wet – minst genomen – voor delen van die uitvoering plaatsvindt zonder legitieme grondslag. De in de Grondwet toegestane inbreuken op het recht op privacy en de communicatievrijheid veronderstellen een uitzondering bij wet. En daarmee wordt niet bedoeld een wet die (deels) strijdig is met het Handvest van de grondrechten van de EU. Minst genomen moet worden aangehouden dat de huidige wettelijke regeling *geen* legitieme grondslag biedt voor bewaring en verstrekking van gegevens, voor zover die verder gaat dan het HvJ EU accepteert. Door aanbieders desalniettemin te verplichten de huidige wettelijke regeling onverkort na te leven, totdat onderhavig wetsvoorstel is aangenomen, brengt de Minister (en als relevante toezichthouder: de Minister van Economische Zaken; uitgevoerd door het AT) aanbieders in een uiterst lastige positie: zij kunnen niet daadwerkelijk controleren in hoeverre de noodzakelijke waarborgen – zoals die voor de overheid in onderhavig voorstel worden aangescherpt – voor informatieverzoeken worden ingevuld en moeten desalniettemin daaraan meewerken. De ontkenning dat dit een probleem zou zijn – door het Ministerie – is in strijd met de onderstreepte woorden in de brief aan de Tweede Kamer.

Het is volgens KPN dan ook minimaal noodzakelijk dat de Minister ervoor zorgt dat de aangescherpte waarborgen voor de bevraging van aanbieders zover als dat mogelijk is met onmiddellijke ingang al wordt ingevoerd. Voor zover dat nog niet zo kunnen – omdat de eis van rechterlijke tussenkomst geen wettelijke grondslag heeft – zal een zeer restrictieve toepassing van de bevraging met extra waarborgen binnen het OM dienen te worden gevolgd. Zonder een dergelijke toezegging en beleidsaanpassing zou de Minister ook naar zijn eigen oordeel mogelijk aanbieders dwingen in strijd te handelen met de Grondwettelijke uitgangspunten. En dat kan in ons rechtsbestel nooit de bedoeling zijn.

Relatie tot Wet bescherming persoonsgegevens

Bij de totstandkoming van de wet bewaarplicht is geen aandacht geschonken aan de relatie tussen het verplicht bewaren van een groot aantal gegevens en het recht op inzage uit de WBP. In het verslag van een schriftelijk overleg[7] wordt aangegeven dat het CBP op dit gebied toezicht houdt en

---

6 *Kamerstukken II* 2014/15, 33 542, nr. 16, p. 7-8.

7 *Kamerstukken II* 2014/15, 33 870, nr. 2, p. 19 en 28-29.

bij onvoldoende naleving van het inzagerecht actie kan ondernemen. Naar het KPN voorkomt is dit onderwerp onvoldoende doordacht. Het inzagerecht is geheel logisch en – als het goed is – in bedrijfsprocessen te implementeren voor het bewaren en verstrekken van persoonsgegevens die een verantwoordelijke (in de zin van de WBP) in het kader van zijn eigen bedrijfsvoering gebruikt. Maar de aanvullende bewaring die voortvloeit uit de wet bewaarplicht leidt ertoe dat een aanbieder veel meer informatie moet opslaan en bewaren dan hij zelf nodig en wenselijk acht. Die informatie moet bovendien beveiligd, afgezonderd en met bijzondere waarborgen worden opgeslagen en bewaard. Bij de specifiek voor dat doel opgeslagen of (langer) bewaarde gegevens gelden de eisen van het Besluit beveiliging gegevens telecommunicatie en de normale processen die een aanbieder inricht om aan zijn inzageplicht te voldoen zijn dan ook niet geschikt en toelaatbaar om voor die specifieke data een inzagerecht te bieden. De bijzondere medewerkers die toegang tot die gegevens hebben zijn echter niet de medewerkers die in het klantproces zitten. En in het kader van de bewaarplicht mag een deel van de vragen van een klant niet eens worden beantwoord, omdat informatie over gebruik en verstrekking van de gegevens valt onder de wettelijke geheimhoudingsplicht.

Kortom: de bewaarplicht creëert een uiterst vervelende situatie, waarin aanbieders beklemd raken tussen twee tegenstrijdige verplichtingen: de transparantieplicht van de WBP en de strafrechtelijk gesanctioneerde geheimhoudingsplicht in her kader van strafvordering en (staats-)veiligheid. De suggestie in de Kamerstukken dat het CBP dit probleem zou kunnen oplossen door *'een modelbrief te publiceren waarmee betrokkenen zich tot hun aanbieder kunnen wenden om hun inzagerecht uit te oefenen'* doet dan ook totaal geen recht aan de aard van dit probleem. Aanbieders worden wettelijk verplicht om ten behoeve van de overheid gegevens te bewaren en beveiligen, maar krijgen als 'tegenprestatie' ook nog verdergaande verplichtingen jegens hun klanten, waarbij de overheid zich op geen enkele wijze er rekenschap van lijkt te geven dat zij in haar opdracht daarmee in een vervelende verhouding tot hun klanten komen te staan.

KPN pleit er daarom voor dat in het kader van het wetsvoorstel dit onderwerp beter wordt doordacht en er passende oplossingen aan de wettelijke regeling worden toegevoegd om de gesignaleerde dilemma's te voorkomen. Aanbieders zouden bij voorkeur hier moeten kunnen volstaan met een algemene beschrijving van hoe het bewaarproces bij hen is ingevuld (na en naast de termijn van bewaring voor de eigen bedrijfsvoering) en voor het overige kunnen volstaan met verwijzing naar de bevoegde instanties. De transparantie over wat er gebeurt met ten behoeve van de overheid bewaarde gegevens zou principieel van die overheid en niet van de aanbieders moeten komen.

Toezicht

Op basis van een bevinding in het WODC rapport – te weten dat volgens het AT controle op de naleving van de wet thans beperkt moet zijn tot 'systeemtoezicht', omdat het AT geen kennis mag nemen van de inhoud van de bewaarde gegevens – wordt artikel in 18.7 volgens het voorstel opgenomen dat aangewezen ambtenaren van het AT wel inzicht in de gegevens moet worden gegeven in het kader van toezicht op deze bepaling. Op het eerste gezicht is het vreemd dat er hiermee dus juist een uitbreiding van de kennisname van de bewaarde gegevens wordt gecreëerd, die niet te maken heeft met de inhoud van die gegevens. Het HvJ EU heeft de kennisneming met het oog op de inhoud al als te ruim geoordeeld en nu wordt zelfs zonder belang bij de inhoud aan een nieuwe categorie ambtenaren een dergelijk recht gegeven. KPN vraagt zich ten zeerste af in hoeverre werkelijk is onderzocht dat het toezicht van het AT feitelijk wordt belemmerd door het ontbreken van een dergelijke bevoegdheid.

Nog een detailopmerking bij de toelichting

Op p. 8-9 van de MvT wordt aangegeven dat teruggaan naar de situatie van voor 2009 niet mogelijk zou zijn omdat in de praktijk dit bijvoorbeeld tot gevolg zou hebben dat veel verkeersgegevens en internetgebruikersgegevens dan direct nadat de communicatie heeft plaatsgevonden vernietigd kan worden. Die opmerking lijkt KPN ver gezocht. Ten aanzien van de categorie telefoniegegevens lijkt er heel weinig te zijn veranderd in de praktijk en het blijkt (ook uit het WODC rapport) dat in de praktijk de bevraging voornamelijk op die categorie gegevens betrekking heeft. Ten aanzien van internetgegevens geldt dat de aanbieders inderdaad een deel van die gegevens niet voor hun bedrijfsvoering nodig hebben, maar voor een deel worden die overbodige gegevens met het wetsvoorstel ook geschrapt. Het belangrijkste wat KPN kan bedenken dat echt een verschil zou maken met de praktijk zonder wet is nu juist de 'vergaarplicht' die ten aanzien van IP adressen en identificatie met dit wetsvoorstel wordt voorgesteld. Die zou er inderdaad zonder wettelijke basis niet zijn. Maar dat was onder de wet van 2009 ook niet het geval.

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank NL32ABNA0554706512
KvK 34121286

M
E
W https://www.bof.nl

Ministerie van Veiligheid en Justitie

Betreft
Reactie op ontwerpwetsvoorstel aanpassing Wet bewaarplicht

Amsterdam
19 december 2014

Geachte heer, mevrouw,

Graag reageert Bits of Freedom op het ontwerpwetsvoorstel[1] voor het aanpassen van de wetgeving op grond waarvan het communicatiegedrag en geografische locatie van vrijwel alle burgers, verdacht of niet, langdurig wordt bewaard. Het gaat om een wijziging van de Wet bewaarplicht telecommunicatie-gegevens, hierna: Wet bewaarplicht.

Inleiding

1. Bits of Freedom is verheugd te zien dat het ministerie eindelijk helder maakt welke conclusies zij aan het baanbrekende vonnis van het Hof van Justitie van de Europese Unie (hierna: Het Hof) verbindt.[2] De regering deelt het standpunt van de Raad van State dat de huidige Wet bewaarplicht in strijd is met de artikelen 7 en 8 van het Handvest van de grondrechten.

2. De minister stelt voor om de toets voorafgaande aan de toegang tot de gegevens iets te verzwaren, de strafbare feiten waarvoor de langst-bewaarde gegevens gevorderd mogen worden in te perken en de opslag van de gegevens op Europees grondgebied af te dwingen.

3. Bits of Freedom is echter van mening dat deze wijzigingen op geen enkele wijze de fundamentele problemen van deze wet oplossen. Ook adresseren

1 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
2 C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger e.a.

ze niet de door het Hof gestelde voorwaarden. Bits of Freedom vindt dan ook dat i) dit ontwerpwetsvoorstel niet verder zou moeten worden uitgewerkt, ii) de Wet bewaarplicht in zijn geheel moet worden ingetrokken en iii) tot die tijd de handhaving van die wet opgeschort moet worden.

We zullen dat in deze brief nader toelichten.

Meest fundamentele probleem wordt niet opgelost: noodzakelijkheidstoets

4. Het ontwerpwetsvoorstel lost het grootste en meest fundamentele probleem niet op: het langdurig en ongericht bewaren van gegevens over het communicatiegedrag en de geografische locatie van voornamelijk onverdachte Nederlanders.

5. Op grond van de Wet bewaarplicht wordt vastgelegd wie wanneer met wie contact heeft gehad, hoe lang dat contact heeft geduurd en wat de geografische locatie was van beide gesprekspartners. De gegevens met betrekking tot het belgedrag worden voor de duur van één jaar bewaard. Omdat ook gegevens over het opzetten en afbreken van internetsessies moeten worden bewaard en internetverbindingen over telefonienetwerken niet erg stabiel zijn, worden ook veelvuldig gegevens over de geografische locatie van de gebruiker opgeslagen als deze niet actief communiceert.

   Op basis van de gegevens zijn zeer intieme details over de gebruiker te achterhalen, waaronder diens sociale netwerk, culturele achtergrond, seksuele voorkeuren, geografische locatie, interesses, maatschappelijke, politieke en religieuze standpunten en soms ook iemands financiële en medische geschiedenis.[3]

   Ook de regering erkent, bij monde van minister van Binnenlandse Zaken, de gevoeligheid van dit soort gegevens: "[...] de toepassing van verfijnde methodieken van metadata-analyse kunnen onder omstandigheden ingrijpender zijn dan een kortstondige interceptie van de inhoud van de telecommunicatie."[4]

6. De Wet bewaarplicht maakt daarmee een enorme inbreuk op verschillende grondrechten van alle Nederlandse burgers, waaronder het recht op het respect van de persoonlijke levenssfeer, het recht op de bescherming van persoonsgegevens en het recht op de vrijheid van meningsuiting. Eén van de voorwaarden die het Europees Verdrag van de Rechten van de Mens aan zulke inbreuken stelt is dat zo'n inbreuk in een democratische samenleving

3 https://decorrespondent.nl/528/Hoe-je-onschuldige-smartphone-bijna-je-hele-leven-doorgeeft-aan-de-geheime-dienst/25712016-b07ce737

4 http://www.rijksoverheid.nl/nieuws/2014/03/11/kabinetsreactie-commissie-dessens-en-ctivd-rapport.html

noodzakelijk moet zijn. Deze noodzakelijkheid is echter nooit aangetoond.[5] [6]

De Nederlandse regering is in de afgelopen paar jaar niet in staat gebleken om de noodzakelijkheid van enkel het bewaren van de gegevens te onderbouwen. Dat kon de regering ook niet na herhaalde vragen daartoe van de Tweede Kamer, de Europese Commissie en belangenorganisaties zoals Bits of Freedom.

Ook het Wetenschappelijk Onderzoeks- en Documentatiecentrum ("WODC") kon in haar evaluatie van de wet de noodzakelijkheid niet aantonen..[7]

Ook bleek uit datzelfde onderzoek dat een aantal van de type bewaarde gegevens eigenlijk nooit worden opgevraagd.[8] Zo worden gegevens over het gebruik van e-mail eigenlijk nooit gevorderd. Bovendien bleek dat het zwaartepunt van de vorderingen in het begin van de bewaartermijn ligt.[9] Daaruit valt af te leiden dat het niet nodig is deze gegevens zo lang te bewaren – voor zover het bewaren al nodig is.

7. Het ontwerpwetsvoorstel adresseert de noodzakelijkheidstoets op geen enkele wijze. Dat betekent dat tenminste een van de meest fundamentele problemen van de Wet bewaarplicht niet wordt opgelost.

<u>Ontwerpvoorstel voldoet ook niet aan andere door het Hof geformuleerde eisen</u>

8. Meer in het bijzonder voldoet het voorstel ook niet aan de voorwaarden die aan een dergelijke inbreuk op de fundamentele grondrechten door de rechters van het Hof zijn geformuleerd.[10]

   Het Hof meent dat de noodzakelijkheid van het op grote schaal bewaren van gegevens over het communicatiegedrag en de geografische locatie van alle burgers, verdachte of niet, niet is aangetoond. Daarnaast stelt het Hof tal van eisen aan het bewaren van, de toegang tot en het gebruik van de gegevens en andere waarborgen. Graag licht ik hieronder toe hoe ook dit ontwerpwetsvoorstel niet voldoet aan deze eisen.

Ongerichtheid van het bewaren van gevoelige gegevens

9. Ten eerste zorgt het ontwerpwetsvoorstel er niet voor dat er een directe relatie bestaat tussen de gegevens die bewaard worden en het doel waarvoor die gegevens bewaard worden. In de huidige Wet bewaarplicht ontbreekt ook zo'n directe relatie. Het ontwerpwetsvoorstel verandert hier

---

5 https://www.bof.nl/2014/02/06/adviseur-regering-kritisch-over-bewaarplicht/
6 https://www.bof.nl/2014/04/16/bewaarplicht-wrong-on-so-many-levels/
7 De Wet bewaarplicht telecommunicatiegegevens, WODC, 2013, pagina 13.
8 De Wet bewaarplicht telecommunicatiegegevens, WODC, 2013, pagina 73 en 76.
9 De Wet bewaarplicht telecommunicatiegegevens, WODC, 2013, pagina 64 en 66.
10 C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger e.a.

niets aan.[11]

10. Ten tweede maakt het ontwerpwetsvoorstel geen uitzondering voor de gegevens die betrekking hebben op beroepsmatige geheimhouders. Gegevens over de communicatie van personen die in hun beroep en om goede redenen verplicht zijn tot geheimhouding, zoals advocaten, artsen, psychiaters en notarissen, wordt dan ook langdurig bewaard.[12]

Toegang tot en gebruik van gegevens onvoldoende gemotiveerd

11. Ten derde ontbreken objectieve grenzen waarmee gewaarborgd wordt dat de toegang en het gebruik van de bewaarde gegevens altijd proportioneel is.[13]

    De huidige Wet bewaarplicht is "begrenst" tot alle misdrijven waarop vier jaar of langer hechtenis staat en ook nog eens vele tientallen andere misdrijven, waaronder zelfs misdrijven waarop slechts een maximale hechtenis van zes maanden (!) is gesteld.

    In het ontwerpwetsvoorstel is dat iets aangepast door vorderingen van gegevens in de periode van zes tot twaalf maanden voorafgaand aan de datum van de vordering alleen nog toe te staan in het geval van verdenking van een zwaar misdrijf. Daarbij moet het gaan om misdrijven waarop een gevangenisstraf van acht jaren of meer is gesteld.

    Er is echter nog altijd geen sprake van objectieve grenzen waardoor de toegang tot de gegevens altijd proportioneel is. Het is op zijn minst noodzakelijk dat de minister deugdelijk motiveert op basis waarvan die grenzen zijn vastgesteld.

Bewaartermijnen zijn niet gebaseerd op objectieve criteria

12. Ten vierde zijn de bewaartermijnen in het ontwerpwetsvoorstel niet gebaseerd op objectieve criteria om te waarborgen dat het beperkt is tot het hoogst noodzakelijke.[14] Immers, het feit dat de gegevens bewaard worden is op zichzelf al een inbreuk op fundamentele grondrechten, ongeacht de vraag hoe de toegang tot en het gebruik van de gegevens is gewaarborgd.

    Het voorstel handhaaft een bewaartermijn van zes maanden voor gegevens gerelateerd aan het gebruik van internet en een heel jaar voor gegevens voor het gebruik van telefonie.

11 C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger e.a., paragraaf 57 en 59.
12 C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger e.a., paragraaf 58.
13 C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger e.a., paragraaf 60.
14 C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger e.a., paragraaf 64.

Het voorstel, noch de toelichting daarop, maakt helder op basis van welke objectieve criteria zeker gesteld is dat de termijn voor het bewaren beperkt is tot het strikt noodzakelijke. Ook hier geldt dat de minister deugdelijk moet motiveren hoe die grenzen zijn vastgesteld.

Bestaande waarborgen werken niet of worden geschrapt.

13. Ten vijfde geldt dat de huidige waarborgen niet functioneren of op termijn worden ingeperkt. Het Hof stelt echter expliciet dat als een betrokkene niet weet dat zijn gegevens bewaard en later gebruikt worden, diegene het gevoel kan krijgen dat hij constant in de gaten wordt gehouden.[15]

    Zo blijkt uit het onderzoek van het WODC dat het recht op inzage in de eigen verkeers- en locatiegegevens in de praktijk niet werkt en daarmee een loze waarborg is.[16]

    Daarnaast heeft uw kabinet een wetsvoorstel gedaan om een andere belangrijke waarborg te schrappen: de verplichting aan het Openbaar Ministerie om de betrokkene te notificeren nadat gegevens over diens communicatiegedrag zijn gevorderd. Maar alleen als de betrokkene op de hoogte is van de inzet van een opsporingsbevoegdheid kan de betrokkene deze toepassing laten toetsen.[17]

<u>Conclusie: de bewaarplicht moet in zijn geheel worden ingetrokken</u>

14. Op grond van de Wet bewaarplicht worden gegevens over het communicatiegedrag en de geografische locatie van alle Nederlanders, verdacht en onverdacht, bewaard voor de duur van één jaar. De wet maakt daarmee een enorme inbreuk op het recht op het respect voor de persoonlijke levenssfeer, het recht op de bescherming van persoons-gegevens en het recht op de vrijheid van meningsuiting. Dit zijn fundamentele mensenrechten, zoals vastgelegd in diverse ons verbindende internationale verdragen. Bits of Freedom acht ongerichte surveillance, en zeker op deze gigantische schaal, ongepast in een democratische rechtsstaat.

15. Bits of Freedom vindt dan ook dat:
    a. dit ontwerpwetsvoorstel niet verder moet worden uitgewerkt,
    b. de Wet bewaarplicht in zijn geheel moet worden ingetrokken en
    c. tot die tijd de handhaving van die wet opgeschort moet worden.

15 C-293/12 en C-594/12,Digital Rights Ireland en Seitlinger e.a., paragraaf 37.
16 De Wet bewaarplicht telecommunicatiegegevens, WODC, 2013, pagina 57.
17 https://www.bof.nl/live/wp-content/uploads/20140312-met-minder-moeite-meer-transparantie.pdf

Ik vetrouw erop u hiermee voldoende te hebben geïnformeerd. Mocht u nog vragen hebben, dan zijn wij vanzelfsprekend bereid een nadere toelichting te geven.

Met vriendelijke groet,

Namens Bits of Freedom

30 januari 2015

Reactie Ziggo op ontwerpwetsvoorstel tot Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten ('conceptwetsvoorstel tot wijziging van de Wet bewaarplicht telecommunicatiegegevens')

Op 18 november 2014 is het Ministerie van Veiligheid en Justitie een consultatie gestart over het conceptwetsvoorstel tot wijziging van de Wet bewaarplicht telecommunicatiegegevens. Het conceptwetsvoorstel is een reactie op het arrest van 8 april 2014 van het Hof van Justitie van de Europese Unie (hierna: het Hof), waarin het Hof de richtlijn 2006/24/EG ongeldig heeft verklaard.

Bij brief van 16 december 2014 (kenmerk 525682) heeft de Directeur Wetgeving en Juridische Zaken, mevrouw A.G. van Dijk, van het Ministerie van Veiligheid en Justitie het conceptwetsvoorstel aan Ziggo en UPC Nederland toegestuurd. De deadline voor reactie op het conceptwetsvoorstel is uiterlijk 1 februari 2015.

Naar aanleiding van de overname van Ziggo B.V. door Liberty Global Plc., het moederbedrijf van UPC Nederland B.V. (definitief op 11 november 2014), kan de onderstaande zienswijze worden beschouwd als de gezamenlijke reactie van Ziggo en UPC Nederland, hierna verder aangeduid als Ziggo. Ziggo stelt het zeer op prijs dat zij in de gelegenheid wordt gesteld om haar zienswijze te geven op het conceptwetsvoorstel.

Ziggo stelt vast dat de Nederlandse regering door middel van het conceptwetsvoorstel een antwoord geeft op de situatie die is ontstaan als gevolg van de uitspraak van het Hof. Naar aanleiding van deze uitspraak is in het conceptwetsvoorstel een aantal wijzigingen ten opzichte van de huidige Wet bewaarplicht telecommunicatiegegevens opgenomen. Zo wordt er o.a. een beperking opgelegd ten aanzien van de toegang tot de gegevens met betrekking tot telefonie over een vast of mobiel netwerk ten behoeve van de opsporing van ernstige misdrijven aan de hand van de ernst van het betreffende misdrijf en is een voorafgaande machtiging van de rechter-commissaris vereist.

Voor Ziggo is echter onduidelijk hoe het conceptwetsvoorstel zich verhoudt tot de uitspraak van de Raad van State in haar voorlichting dat de huidige Wet bewaarplicht telecommunicatiegegevens in zijn huidige vorm niet in stand kan blijven wegens strijd met het Unierecht.[1] Aangezien het nog enige tijd zal duren voordat het nieuwe voorstel in werking zal treden, is het voor Ziggo onduidelijk of, en zo ja, op welke wijze de huidige wet nog van toepassing is en zal worden gehandhaafd. Het spreekt voor zich dat juist het antwoord op deze vraag van groot belang is voor Ziggo met het oog op de activiteiten en investeringen die Ziggo moet uitvoeren om te voldoen aan de in de wet opgenomen verplichtingen ten aanzien van het opslaan van gegevens.

Daarnaast krijgt Ziggo met enige regelmaat vragen van haar klanten over de huidige ontstane situatie waarop vooralsnog door haar niet een eenduidig antwoord te geven is.

[1] Raad van State, Advies W03.14.0161/II/Vo, donderdag 17 juli 2014 (citaat): *"De wet bewaarplicht telecommunicatiegegevens kan als zodanig niet in stand blijven wegens strijd met het Unierecht."*

Tevens is het voor Ziggo niet duidelijk waarom de Nederlandse regering in het conceptvoorstel vast blijft houden aan de bestaande bewaartermijnen voor internetgegevens (zes maanden) en telefoniegegevens (twaalf maanden), terwijl het Hof in haar uitspraak van mening is dat een vergaande, onbeperkte en algemene plicht tot opslag van gegevens niet gerechtvaardigd is. De bewaarplicht moet, aldus het Hof, beperkt zijn tot wat strikt noodzakelijk is en er moeten duidelijke en precieze regels worden gesteld. Juist het feit dat de richtlijn dataretentie algemeen van toepassing is op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld, of enige uitzondering wordt gemaakt op basis van het doel, criminaliteit te bestrijden, heeft er toe geleid dat het Hof de richtlijn ongeldig heeft verklaard.

Het is de vraag of de oplossing die de Nederlandse regering kiest, namelijk het in stand houden van de huidige opslagtermijnen van gegevens van alle burgers, maar het beperken van de toegang tot deze gegevens aan de hand van de ernst van het betreffende misdrijf, voldoende recht doet aan de kritiek van het Hof.[2] Het standpunt van de Nederlandse regering laat onverlet dat de toegang van internetgegevens gedurende een periode van zes maanden nog steeds ongeconditioneerd is. Daarnaast wordt in de toelichting bij het conceptwetsvoorstel de verplichte opslag van verkeersgegevens en internetgebruikersgegevens gerechtvaardigd op basis van de stelling dat – anders dan in 2009 bij de totstandkoming van de Wet bewaarplicht telecommunicatiegegevens – het nu bij veel contracten als gevolg van de technologische ontwikkelingen niet meer noodzakelijk is om voor bedrijfsdoeleinden verkeersgegevens en internetgebruikersgegevens te bewaren.[3] Derhalve is volgens de Nederlandse regering een wettelijke bewaarplicht voor deze gegevens noodzakelijk. Voor Ziggo is onduidelijk wat met deze zin wordt bedoeld. Een nadere toelichting op dit punt is wenselijk.

Tenslotte geeft de Nederlandse regering in de toelichting op het conceptwetsvoorstel aan dat het wetsvoorstel tevens gevolgen zal kunnen hebben voor de bedrijfsvoering en de kosten van de in Nederland opererende internet- en telecomaanbieders. De Nederlandse regering stelt dat de precieze bedrijfseffecten en kosten in samenwerking met het bedrijfsleven in kaart zullen worden gebracht. Het spreekt vanzelf dat Ziggo gaarne bereid is om op dit punt met de Nederlandse regering samen te werken, waarbij dient te worden opgemerkt dat opslag van gegevens op het grondgebied van de Europese Unie op voorhand niet de enige mogelijke additionele kostenpost voor internet- en telecomaanbieders behoeft te zijn. Niet valt uit te sluiten dat de door de Nederlandse regering voorgestelde aanpassing van de bijlage behorende bij artikel 13.2a van de Telecommunicatiewet ook gevolgen heeft voor de bedrijfsvoering en de kosten van de aanbieders.

---

[2] De Nederlandse regering stelt in haar brief van 17 november 2014 aan de Tweede Kamer ('Reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie') in paragraaf 5.3.1 Eisen aan de wetgeving (citaat): *"In het licht hiervan dient de desbetreffende overweging van het Hof van Justitie naar het oordeel van de regering zo te worden uitgelegd, dat het feit dat de richtlijn geen enkel verband vereist tussen de opslag van gegevens en het gedrag van personen, weliswaar een zeer vergaande inbreuk op de persoonlijke levenssfeer van de betrokkenen kan vormen, maar dat de ernst van die inbreuk kan worden gematigd door het opnemen van passende garanties en waarborgen voor een zorgvuldige wijze van bewaren en verwerken van gegevens, alsmede de toegang tot die gegevens."*

[3] Memorie van Toelichting bij het conceptwetsvoorstel, paragraaf 4. De noodzaak van een bewaarplicht voor de opsporing en vervolging van ernstige misdrijven (citaat): *"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."*

0 BD

PLATFORM BOD
BIJZONDERE OPSPORINGSDIENSTEN

Platform Bijzondere Opsporingsdiensten

Fiscale Inlichtingen- en Opsporingsdienst
Bernadottelaan 13
3527 GA Utrecht
Postbus 19266
3501 DG Utrecht

Secretariaat Platform BOD-en

Ministerie van Veiligheid en Justitie
T.a.v. de heer LW. Opstelten
Minister van Veiligheid en Justitie
Postbus 20301
2500 EH Den Haag

Uw kenmerk -
Ons kenmerk
Betreft Ontwerp-wetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens

Datum
28 januari 2015

Bijlagen
1

Zijne Excellentie,

Op 18 november 2014 heeft u een internetconsultatie opengesteld voor het ontwerp-wetsvoorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten. Anders dan gebruikelijk zijn wij niet per brief verzocht om consultatie. In afstemming met uw Directie Wetgeving en Juridische Zaken is de termijn voor reactie van het Platform Bijzondere Opsporingsdiensten verruimd naar 1 februari 2015.

Namens de leden van het Platform Bijzondere Opsporingsdiensten maak ik graag van de gelegenheid gebruik een reactie te geven op genoemd ontwerp-wetsvoorstel. Onze reactie treft u in de bij deze brief gevoegde bijlage aan.

Graag worden wij op de hoogte gehouden over de verdere voortgang.

Met vriendelijke groet,

De Voorzitter Platform Bijzondere Opsporingsdiensten

Directeur FIOD

Het Platform Bijzondere Opsporingsdiensten is het samenwerkingsverband van de vier bijzondere opsporingsdiensten, het Functioneel Parket van het Openbaar Ministerie, de Dienst Landelijke Recherche van de Nationale Politie, Koninklijke Marechaussee, Rijksrecherche en het Ministerie van Veiligheid en Justitie.

Bijlage 1

Reactie Platform Bijzondere Opsporingsdiensten inzake Ontwerp-wetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens

---

Betreft: ontwerp-wetsvoorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten.

Inleiding
Op 8 april 2014 heeft het Hof van Justitie van de Europese Unie Richtlijn 2006/24/EG (hierna: de dataretentierichtlijn) ongeldig verklaard wegens strijd met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie[1]. De ongeldigverklaring geldt met terugwerkende kracht voor de gehele richtlijn. De dataretentierichtlijn is in Nederland geïmplementeerd via de Wet bewaarplicht telecommunicatiegegevens. Op verzoek van de minister van Veiligheid & Justitie, heeft de Afdeling advisering van de Raad van State op 7 juli 2014 de mogelijke gevolgen van het arrest voor de nationale wetgeving voorgelicht. Bij brief van 17 november 2014 heeft het Kabinet de Tweede Kamer hierover geïnformeerd. Hierbij blijkt dat de bewaarplicht in Nederland als zodanig blijft bestaan, maar wel met meer waarborgen wordt omkleed. Daartoe is een voorstel tot wijziging van het Wetboek van Strafvordering en van de Telecommunicatiewet ter consultatie voorgelegd. Het College Bescherming persoonsgegevens zal hierover advies geven.

Advisering BOD-en
Voor het wetsvoorstel dat onderwerp is van dit advies is het Platform Bijzondere Opsporingsdiensten niet benaderd voor een advisering. Dit heeft tot gevolg dat de eventuele noties via een internet-consultatie kenbaar moeten worden gemaakt. De termijn van die consultatie is inmiddels verstreken (uiterlijke datum 31 december 2014). In afstemming met de Directie Wetgeving en Juridische Zaken van het Ministerie van Veiligheid en Justitie is de termijn voor reactie van het Platform Bijzondere Opsporingsdiensten verruimd naar 1 februari 2015.

Dataretentierichtlijn
De dataretentierichtlijn heeft betrekking op het bewaren van telecommunicatiegegevens en kwam in 2006 tot stand in reactie op de terreuraanslagen in Londen van 2004 en Madrid van 2005. De richtlijn draagt de lidstaten op, om aanbieders van telecommunicatiediensten bepaalde categorieën gegevens verplicht te laten te bewaren door telecomaanbieders en aan rechtshandhavingsautoriteiten beschikbaar te stellen voor de bestrijding van terrorisme en ernstige criminaliteit. Dit betreft kort gezegd gebruikers-/ verkeersgegevens (inclusief locatiegegevens) van vaste telefonie, mobiele telefonie, sms, internet en e-mail. De lidstaten kunnen een bewaartermijn opleggen van tussen de zes maanden en twee jaar. In Nederland geldt voor telefonie een bewaartermijn van een jaar en voor internet een bewaartermijn van een half jaar.

Uitspraak Europees Hof van Justitie
Volgens het Hof is de dataretentierichtlijn in strijd met artikel 7 (recht op privacy) en 8 (recht op bescherming persoonsgegevens) van het Europese Handvest van de grondrechten. Deze artikelen sluiten aan op de inhoud van artikel 8 van het Europees Verdrag voor de Rechten van de Mens. Het Hof stelt in haar uitspraak vast, dat de te bewaren telecommunicatiegegevens in hun geheel beschouwd zeer nauwkeurige aanwijzingen geven over het privéleven van de betrokkene. Door het bewaren daarvan verplicht te stellen en de toegang toe te staan aan de nationaal bevoegde autoriteiten, is

---

[1] Arrest van 8 april 2014 in de gevoegde zaken C-293/12 (Digital Rights Ireland tegen Ierland) en C-594/12 (Seitlinger, Tschohl e.a. tegen Kärntner Landesregierung).

er sprake van een ernstige inmenging in de fundamentele recht op eerbiediging van het privéleven en bescherming van persoonsgegevens. Een dergelijke inmenging kan onder voorwaarden gerechtvaardigd zijn, maar het Hof oordeelt ten aanzien van de richtlijn dat de vereiste evenredigheid ontbreekt. Hierbij speelt ondermeer een rol dat de in de richtlijn omschreven bewaarplicht geen onderscheid maakt tussen personen en gegevens en de bewaartermijn niet wordt gerechtvaardigd. De bewaarplicht beperkt zich namelijk niet tot personen die in aanraking zijn met een mogelijk strafbaar feit, een bepaald tijdsbestek, geografische zone of kring tot personen, met het beroepsgeheim wordt geen rekening gehouden en er is geen direct verband is tussen bewaarde gegevens en bedreiging van de openbare orde/veiligheid.

Concept wetsvoorstel
De regering heeft voorgesteld om de Telecommunicatiewet en het Wetboek van Strafvordering naar aanleiding van de uitspraak als volgt aan te passen:
de vordering van de officier van justitie tot het verstrekken van door Telecommunicatiewet aanbieders bewaarde historische telecommunicatiegegevens kan slechts worden gegeven na een voorafgaande machtiging door de rechter-commissaris (wijziging van de regeling van artikel 126n/u van het Wetboek van Strafvordering);
de toegang tot de gegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven wordt gedifferentieerd aan de hand van de ernst van het misdrijf (wijziging van de regeling van artikel 126n/u van het Wetboek van Strafvordering);
de aanbieders van telecommunicatiediensten worden verplicht de te bewaren gegevens op het grondgebied van de Europese Unie te bewaren (wijziging artikelen 13.2a en 13.5 van de Telecommunicatiewet);
Agentschap Telecom kan als toezichthoudende autoriteit inzage krijgen in telecommunicatiegegevens die door de aanbieders worden bewaard of verstrekt, met het oog op een beter toezicht op de verwerking van de te bewaren gegevens, en de vernietiging daarvan (wijziging van artikel 18.7, tweede lid, van de Telecommunicatiewet).

Nut en noodzaak telecommunicatiegegevens voor de opsporingspraktijk
Het bewaren van verkeers- en gebruikersgegevens is cruciaal voor de bestrijding van ernstige misdrijven. Dergelijke gegevens zijn onmisbaar voor het identificeren van een gebruiker, het vaststellen van de relaties, plaatsbepaling, of voor het maken van een proportionaliteit, subsidiariteits- en capaciteitsafweging voor de inzet van zwaardere opsporingsmiddelen.

Dat de gebruikers- en verkeersgegevens een meerwaarde hebben, wordt door het Europese Hof van Justitie erkend. Deze onderhavige gegevens bevatten geen informatie over de inhoud van de communicatie. Die inhoud kan (door middel van interceptie) slechts worden verkregen na voorafgaande machtiging van de Rechter-Commissaris. Een dergelijke machtiging wordt uitsluitend verstrekt, als er sprake is van een verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten en er sprake is van een ernstige inbreuk op de rechtsorde.

De gebruikers- en verkeersgegevens zijn onlosmakelijk met elkaar verbonden. Een juiste interpretatie van de verkeersgegevens kan niet worden gedaan zonder de beschikking te hebben over de gegevens van de gebruikers. Zonder die laatste gegevens neemt de bruikbaarheid van de verkeersgegevens in aanmerkelijke mate af. Zo is het zonder gebruikersgegevens ondoenlijk om de juiste gebruiker en de juiste aanbieder te achterhalen. Communicatie is vluchtig en ook de gebruikers zijn vluchtig. Het van "de wieg tot het graf" bij één aanbieder van een communicatiedienst blijven is niet meer van deze tijd.

Dat de bevoegdheid van het opvragen van historische gebruikers- en verkeersgegevens onmisbaar is voor opsporingsonderzoeken zal geïllustreerd worden met

voorbeeldcasussen met name op het terrein van (fiscale) fraude. Deze zijn opgenomen in de bijlage van deze brief.

De inbreuk op de privacy door OM en BOD-en
Het bewaren van gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker, levert uiteraard een inbreuk op de privacy op. Deze inbreuk wordt niet veroorzaakt door handelen van de zijde van de opsporingsdiensten of van het openbaar ministerie, immers op het moment dat een aanbieder van een communicatiedienst gegevens bewaart, heeft enkel die aanbieder de beschikking over die gegevens.

Een opsporingsdienst kan niet eerder de beschikking krijgen over de gegevens dan nadat zij het vermoeden heeft dat er een relatie bestaat tussen een gebruiker en een mogelijk gepleegd strafbaar feit. En niet zo maar een strafbaar feit, maar een ernstig strafbaar feit. Een misdrijf waarvoor de wetgever heeft bepaald dat voorlopige hechtenis van toepassing is. Daarnaast moeten de gegevens van belang zijn voor het onderzoek. Tenslotte is er de waarborg van de toets van de officier van justitie. Deze beoordeelt op basis van proportionaliteit en subsidiariteit of het opportuun is dat van de aanbieder van een communicatiedienst gegevens worden gevorderd. Een vordering die alleen door hem gedaan mag worden. De vordering en resultaten daarvan zijn transparant, immers de officier van justitie doet proces-verbaal opmaken (het vierde lid van artikel 126n/u WvSv).

Samenvattend kan geconcludeerd worden dat de inbreuk op de privacy van de burger bij toepassing van de bijzondere opsporingsbevoegdheid van het vorderen van gebruikers- en verkeersgegevens door de officier van justitie beperkt is. Daarbij moet een eerder opmerking herhaald worden: gebruikers- en verkeersgegevens hebben geen betrekking op de inhoud van de communicatie.

Voorstel tot wijziging van artikelen 126n/u van het Wetboek van Strafvordering
De aanpassing van het Wetboek van Strafvordering betreft de beperking van de bevoegdheid van de officier van justitie tot het vorderen van historische verkeersgegevens bij Telecommunicatiewet-aanbieders (art. 126n/u Sv). Voorgesteld wordt dat een dergelijke vordering slechts kan worden gedaan na voorafgaande rechterlijke toetsing: in de wet zal het vereiste van een voorafgaande machtiging van de RC worden opgenomen. Dit houdt verband met de voorlichting van de Raad van State naar aanleiding van de uitspraak, waaruit blijkt dat: *de toegang van de nationale autoriteiten tot de gegevens op zo'n manier begrensd zal moeten zijn dat alleen die personen toegang krijgen tot de gegevens voor wie dit strikt noodzakelijk is om ernstige criminaliteit te voorkomen, op te sporen of te vervolgen. Hun toegang moet worden onderworpen aan voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie op grond van een gemotiveerd verzoek van de nationale autoriteiten.*

Daarnaast wordt in het Wetboek van Strafvordering de regeling van de toegang van de bewaarde telefoniegegevens nog op een andere manier beperkt. Bij een verdenking van een feit waarvoor voorlopige hechtenis mogelijk is, kan de vordering van de bewaarde gegevens slechts betrekking hebben op een periode van zes maanden voorafgaand aan de datum van de vordering. 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 verkregen. 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 internetgegevens, vanwege de kortere bewaartermijn voor deze gegevens, te weten zes maanden.

Het Platform heeft moeite met de aanpassingen v.w.b. de beperking in de periode waarover de gegevens mogen worden opgevraagd alsook de inmenging van de RC, en wel om de volgende redenen. Zoals hiervoor gememoreerd, is het vorderen van gebruikers- en verkeersgegevens van personen die in een zekere relatie staan tot een verdenking van een ernstig misdrijf een relatief lichte inbreuk op de privacy. Een lichte inbreuk omdat de gebruikers- en verkeersgegevens worden bewaard door een aanbieder van een openbaar communicatiedienst en alleen in uitzonderlijke gevallen van de aanbieders mogen worden gevorderd (bij ernstige misdrijven en via een toets door de officier van justitie). Het is dan ook verwonderlijk dat nu voor zo'n relatief lichte inbreuk de toets door de rechter-commissaris wordt geïntroduceerd.

Een toets door de rechter-commissaris betekent onder andere een administratieve lastenverzwaring voor het openbaar ministerie. In tijden dat onder initiatief van het ministerie van Veiligheid & Justitie getracht wordt om de administratieve lasten te verminderen, komt een dergelijke verzwaring niet logisch over. Het voorstel betekent niet alleen een administratieve lastenverzwaring voor het OM, maar ook voor de kabinetten RC. Het aantal vorderingen op jaarbasis bedraagt ongeveer 46.000. Het moeten verwerken van een dergelijk aantal vorderingen zal - voor zover uit onze positie te beoordelen - gelet op de huidige werklast van de rechters-commissarissen, leiden tot vertraging in de onderzoeken, het oplopen van de doorlooptijden van de strafzaken en de effectiviteit/efficiency van de opsporing negatief beïnvloeden.

De voorgestelde toets betekent een breuk met het huidige toetsingskader in het Wetboek van Strafvordering. Een kader geïntroduceerd met de inwerkingtreding van de Wet bijzondere opsporingsbevoegdheden en de Wet vorderen gegevens. Een kader waarbij het uitgangspunt is dat naar mate de inbreuk op de privacy - door toepassing van bepaalde bevoegdheden - groter wordt, de gevallen waarin die bevoegdheden toegepast mogen worden ernstiger moeten zijn, de voorwaarden strenger worden en toets door rechter noodzakelijk wordt. Het introduceren van de toets door de rechter-commissaris voor niet-inhoudelijke gegevens, terwijl de officier van justitie de bevoegde autoriteit blijft voor meer inbreuk op de privacy makende opsporingsbevoegdheden, is een breuk met het hiervoor geschetste kader.

Ten behoeve van de opsporingsonderzoeken mogen slechts gegevens gevorderd worden over een periode van 6 of 12 maanden: 6 maanden voor de artikel 67 lid 1 WvSv feiten met maximale strafbedreiging tot 8 jaar en 12 maanden voor de strafbedreigingen vanaf 8 jaar. Het gros van de feiten die BOD'en opsporen, kent een maximale strafbedreiging van minder dan 8 jaar. Feiten genoemd in de Wet economisch delicten, valsheid in geschrifte, gekwalificeerde valsheid, oplichting, witwassen, fiscale delicten en milieudelicten zijn daar voorbeelden van. In bijna gevallen gaat het om feiten die (ver) in de historie gepleegd zijn en waarbij de opsporingsdiensten terug moeten rechercheren om bewijs te kunnen vergaren.

Een beperking van te bevragen periode tot 6 maanden voor het vorderen van gebruikers- en verkeersgegevens betekent een forse tegenslag voor de bestrijding van de financieel-economische criminaliteit. Een tegenslag die haaks staat op de wens van de wetgever om die vorm van criminaliteit slagvaardiger aan te pakken. In dit verband wordt verwezen naar de Wet verruiming mogelijkheden bestrijding financieel-economische criminaliteit (gedeeltelijk in werking getreden op 1 januari 2015).

Het merendeel van de bijzondere opsporingsbevoegdheden kunnen op basis van een mondelinge vordering of bevel uitgevoerd worden. Zo ook het met behulp van een technisch hulpmiddel opnemen van niet voor publiek bestemde communicatie (tappen).

Het is dan vreemd dat vorderingen die een lichtere inbreuk op de privacy veroorzaken (het vorderen verkeersgegevens) uitsluitend schriftelijk mogen plaatsvinden. Een gelijkschakeling van de uitvoeringsmogelijkheden van deze interceptie-bevoegdheden is meer dan evident.

Telecommunicatiewet
Communicatie door gebruikmaking van internet technologie wordt steeds belangrijker ten koste van de traditionele telefonie. De verwachting is zelfs zo dat traditionele telefonie binnen afzienbare termijn geheel zal verdwijnen en plaats zal maken voor (mobiele) internettelefonie. Uitgaande van die ontwikkeling is het vreemd dat de bewaartermijn van internet(telefonie)gegevens (verwoordt in artikel 13.2a lid 3 onder b van de Telecommunicatiewet) niet gelijk wordt getrokken met de bewaartermijn van telefonie over een vast of mobiel netwerk (12 maanden). Met een gelijkschakeling wordt het -indien de zwaarte van het te onderzoeken strafbare feit daartoe aanleiding geeft (strafbedreiging van acht jaar of meer)- mogelijk om de gegevens die betrekking hebben op al het "gesproken woord" dat via een communicatiedienst wordt gevoerd over een periode van 12 maanden op te vragen.

Conclusie
Het vorenstaande geeft overduidelijk weer dat voor een effectieve criminaliteitsbestrijding op terreinen van fiscaliteit, voedselveiligheid, arbeidsuitbuiting, milieu, (niet)ambtelijke corruptie en diverse vormen van fraudes het van groot belang is dat de artikelen 126 n en u in haar huidige vorm blijven gehandhaafd. Niet alleen gehandhaafd, maar worden uitgebreid met de mogelijkheid van het mondeling vorderen.

Bijlage

Voorbeeldcasussen (met name (fiscale) fraude) gebruik gegevens als bedoeld in de artikelen 126 n/u van het Wetboek van Strafvordering

Hierna volgen enkele voorbeelden van diverse zaken waarbij het gebruik van data uit het verleden van wezenlijk belang is geweest voor het kunnen uitvoeren van het strafrechtelijk onderzoek.

Daarbij dient het volgende te worden opgemerkt:
De start van een strafrechtelijk onderzoek naar financieel economische- en fiscale fraude is meestal enige tijd nadat deze fraude heeft plaatsgevonden. Alvorens de fraude wordt geconstateerd zijn er meestal al maanden verstreken. Een half jaar is daarbij geen uitzondering. In met name toeslagonderzoeken is het van belang dat gegevens over een langere periode kunnen worden verkregen. Nadat onjuiste aanvragen zijn ingediend gaat er meestal geruime tijd overeen voordat de Belastingdienst middels haar controlesysteem ontdekt dat er sprake is van fraude. In feite geldt dit ook voor BTW-fraude onderzoeken.

De beperkte bewaartermijn van de verkeersgegevens en in het bijzonder IP-adressen is voor deze onderzoeken in zijn algemeenheid een probleem. IP-adressen zijn tegenwoordig van groot belang in (fraude)onderzoeken om te kunnen achterhalen vanaf welke aansluiting een document (belastingaangifte, toeslagaanvraag e.d.) is verstuurd en om na te gaan of er sprake is van structurele fraude vanaf dat IP-adres. Ook voor het kunnen koppelen van verdachten aan andere verdachten of aan de frauduleuze handelingen zijn deze gegevens van essentieel belang. Door de voorgestelde beperking voor het opvragen van gegevens is de kans dat er gegevens worden gemist groot hetgeen de bewijspositie uitermate doet verzwakken.

Ter illustratie kunnen de volgende casussen dienen:
1.
Twee belastingdienstmedewerkers waren betrokken bij het opzettelijk doen van onjuiste aangifte omzetbelasting. Vanuit hun functie konden zij er voor zorgen dat een groep verdachten die de onjuiste aangifte deed, niet werden geselecteerd voor nadere controle wegens afwijkende (te hoge) bedragen in de aangifte. Door het raadplegen van telefoon-printgegevens bij de provider kon, naar aanleiding van 1 contact , beide medewerkers worden gelinkt aan de verdachten.

2.
Op basis van een proces-verbaal van het Team Criminele Inlichtingen (TCI) is een onderzoek gestart naar accijnsfraude in de oliehandel. In dit TCI-proces-verbaal met zeer summiere informatie stond een telefoonnummer. Door het opvragen van historische printgegevens kon het telefoonnummer gekoppeld worden aan een persoon waarna het onderzoek kon worden gestart. Betrof printlijstgegevens van meer dan een half jaar terug.

3.
Via Internet waren 600 valse aanvragen Kinderopvangtoeslag ingediend voor in totaal 10 miljoen euro. Door de IP (internet)adressen te bevragen kon worden aangetoond dat de aanvragen feitelijk gedaan waren door personen die niets te maken hadden met de persoon op wiens naam de aanvraag was gedaan. Tijdens de terechtzitting was het sterkste bewijs het feit dat de aanvragen zowel vanaf een IP adres van de ene verdachte als dat van andere verdachten gedaan werden waardoor er wel sprake moest zijn van verregaande samenwerking. Zonder de IP bevragingen was deze zaak nooit bewezen. Het maximaal een half jaar terug kunnen bevragen van de IP adressen heeft er helaas voor gezorgd dat niet alle aanvragen aan de verdachten konden worden gekoppeld.

4.
Dit onderzoek betrof een BTW-carrousel. Meerdere BV's leveren goederen (veelal op papier) waarbij door een van de BV's de BTW niet wordt afgedragen. Het geld verdwijnt in de zakken van anderen. De BV die niet afdraagt gaat veelal failliet en daardoor loopt de Staat de BTW mis. Door in het verleden te kijken welke personen contact met elkaar hebben gehad kon het netwerk worden blootgelegd.
Voor dat dergelijke praktijken aan het licht komen is er doorgaans minimaal een halfjaar tot een jaar verstreken. In sommige gevallen is de fraude alweer gestopt. Voor het uitvoeren van het strafrechtelijk onderzoek is het van essentieel belang om vast te stellen welke schakels in het verleden rechtstreeks met elkaar contact hebben gehad. Doorgaans langer dan een half jaar terug.

5.
Dit betrof een fraudeonderzoek waarin postbezorgers betrokken waren.
Na het vaststellen van de identiteit van de hoofdverdachte bleek hij onvindbaar (illegaal, geen werk of inkomen bekend, geen actueel woonadres bekend). Wel kwamen uit de telefoons van mede-verdachten telefoonnummers die aan hem te koppelen waren. Hij bleek echter ongeveer eens per maand van telefoonnummer te wisselen. Uit de printlijst van zijn eerste nummer zijn de meest gebelde nummers gedestilleerd, vervolgens zijn hiervan printlijsten opgevraagd, die leidden tot zijn nieuwe(re) nummer. Ook hier is een printlijst van opgevraagd (en dit dus nog driemaal), waarna uiteindelijk het actuele telefoonnummer van de hoofdverdachte kon worden vastgesteld. Na vaststelling van het actuele telefoonnummer is een tap geplaatst en is een IMSI-catcher ingezet, met ondersteuning van het Observatie Team. Dit heeft uiteindelijk geleid tot lokaliseren en aanhouden van de verdachte.

6.
In deze zaak ging het om een handel met voorwetenschap. Tussen moment van constateren en moment dat de aangifte bij de opsporing binnen kwam was ongeveer een half jaar verstreken. Printlijsten korter dan zes maanden terug zijn dan ook niet heel waardevol. Voor het leggen van relaties tussen personen was het in deze zaak van belang om printlijsten van ook langer dan een half jaar oud op te vragen. Zonder deze gegevens was het op zijn minst veel moeilijker geweest om personen aan elkaar te linken.

7.
Een onderzoek naar de handel in illegaal vuurwerk was gestart n.a.v. een TCI proces-verbaal met daarin slechts de tip dat via een website illegaal vuurwerk werd aangeboden. Slechts door het opvragen van internetgegevens kon een pre-paid telefoonnummer worden achterhaald. Via de printgegevens van dit nummer kon de verdachte worden getraceerd.

8.
Door de Rijksrecherche wordt onder meer onderzoek gedaan naar lekken van informatie (art. 272 WvSr; strafbedreiging van max één jaar gevangenisstraf). In de meeste gevallen is het noodzakelijk dat er printlijsten worden opgevraagd over een periode die ouder is dan een half jaar. Zo kon in een strafzaak een door de verdediging geponeerde scenario weerlegd worden door gebruik te maken van historische gegevens van 11 maanden en 2 dagen oud.

0 BD

COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN De minister van Veiligheid en Justitie
De heer mr. I.W. Opstelten
Postbus 20301
2500 EH DEN HAAG

DATUM 10 februari 2015
ONS KENMERK
CONTACTPERSOON

administratie@cbpweb.nl
UW BRIEF VAN 18 november 2014
UW KENMERK

ONDERWERP Wetgevingsadvies Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische telecommunicatiediensten

Geachte heer Opstelten,

Bij brief van 18 november 2014 heeft u, mede namens de minister van Economische Zaken, het College bescherming persoonsgegevens (CBP) op grond van het bepaalde in artikel 51, tweede lid van de Wet bescherming persoonsgegevens (Wbp) gevraagd te adviseren op het wetsvoorstel Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische communicatiediensten (hierna: het wetsvoorstel).

Het wetsvoorstel was ter consultatie opengesteld via internet van 18 november tot en met 31 december 2014. Na ommekomst van de consultatietermijn heeft het ministerie van Veiligheid en Justitie het CBP bericht dat er geen voor het CBP relevante wijzigingen zullen worden doorgevoerd in het wetsvoorstel. Het CBP adviseert derhalve op het wetsvoorstel zoals dat op 18 november 2014 aan het CBP is voorgelegd en voldoet hiermee aan uw verzoek.

Inhoud van het wetsvoorstel

Het wetsvoorstel betreft een aanpassing van de bestaande bewaarplicht voor telecommunicatiegegevens van zowel telefoon- als internetverkeer. De directe aanleiding is het arrest van het Hof van Justitie van de Europese Unie (hierna: het Hof) van 8 april 2014 in de gevoegde zaken Digital Rights Ireland en Seitlinger (hierna: het Hofarrest) waarin de Europese dataretentierichtlijn 2006/24/EG ongeldig is verklaard.

De Nederlandse regering heeft de afdeling Advisering van de Raad van State gevraagd om voorlichting te geven over de gevolgen van het Hofarrest voor de Nederlandse implementatiewetgeving van de ongeldig verklaarde Europese richtlijn (de Wet bewaarplicht telecommunicatiegegevens uit 2009). De Raad van State concludeert dat het enkele feit dat de Europese richtlijn ongeldig is verklaard geen gevolgen heeft voor de geldigheid van de Nederlandse implementatiewetgeving. Tegelijkertijd stelt de Raad dat aangenomen moet worden

dat ook de implementatiewetgeving, die materieel grotendeels overeenkomt met de ongeldig verklaarde richtlijn, strijdig is met artikel 7 en 8 van het Handvest van de Grondrechten van de Europese Unie (hierna: het Handvest). De Wet bewaarplicht telecommunicatiegegevens zal daarom in elk geval moeten worden aangepast om te voldoen aan de in het Hofarrest gestelde voorwaarden.

Het wetsvoorstel behelst geen intrekking van de bewaarplicht telecommunicatiegegevens, maar omvat aanpassingen op de volgende punten.

1. Introductie van een voorafgaande toetsing door een rechter-commissaris op vorderingen van officieren van justitie tot verstrekking van historische telecommunicatiegegevens.
2. Introductie van een onderscheid tussen een bewaartermijn van twaalf maanden voor telefoniegegevens en de termijn van raadpleging ervan tussen de zes en twaalf maanden, afhankelijk van de aard van het misdrijf.
3. Introductie van een verplichting tot opslag en verwerking van de gegevens binnen de Europese Unie.
4. Introductie van een recht op toegang tot de bewaarde gegevens door de toezichthouder.
5. Aanpassing van de bijlage met de specificatie van de te bewaren gegevens.

Beoordeling van het voorstel

Het CBP heeft de inhoud van het wetsvoorstel getoetst aan de normen van noodzakelijkheid, subsidiariteit en proportionaliteit, afkomstig uit artikel 8 van het Europees Verdrag van de Rechten van de Mens, en de artikelen 7 en 8 van het Handvest. Zoals in de bijlage bij deze brief is uiteengezet, luidt zijn oordeel en vervolgens zijn advies hierover als volgt.

Het CBP constateert dat de feitelijke onderbouwing in het wetsontwerp van de noodzaak om de telecommunicatiegegevens van *de facto* elke Nederlander gedurende zes tot twaalf maanden te bewaren, tekort schiet. Het wetsvoorstel bevat geen systematisch, met het gewicht van de voorgestelde maatregel overeenkomend, betoog over de noodzaak voor deze bewaarplicht. Dit terwijl de opsporingsautoriteiten ruim vier en half jaar ervaring hebben kunnen opdoen met de bewaarde persoonsgegevens sinds de inwerkingtreding van de Wet bewaarplicht telecommunicatiegegevens. Het wetsvoorstel bevat in het geheel geen uitwerking van de subsidiariteitstoets.

Ten aanzien van de evenredigheid van het wetsvoorstel stelt het CBP vast dat er geen wezenlijke veranderingen worden aangebracht in het principe van een algemene bewaarplicht. De bewaarplicht wordt niet ingekaderd en kán volgens de regering ook niet worden ingekaderd tot enkel die gegevens die noodzakelijk zijn voor het bestrijden van zware criminaliteit. De inbreuk op de artikelen 7 en 8 van het Handvest is daarmee te groot en voldoet bovendien niet aan het proportionaliteitsvereiste van artikel 8 EVRM.

Ook ten aanzien van de naleving van de notificatieplicht, de controle op het gebruik van de bewaarde gegevens en het ontbreken van uitzonderingen voor mensen met een beroepsgeheim, voldoet het wetsvoorstel niet aan de proportionaliteitsvereisten.

Ten slotte beoordeelt het CBP het door de regering beoogde onderscheid tussen het bewaren van gegevens en het gebruik ervan. Dit onderscheid leidt niet tot beëindiging van de geconstateerde onevenredigheid en daarmee onrechtmatigheid van een algemene bewaarplicht verkeersgegevens. In zijn algemeenheid merkt het CBP in dit verband op dat noch in internationale verdragen, noch in de Wet bescherming persoonsgegevens ruimte is te vinden voor dit beoogde onderscheid.

Advies

Het CBP heeft bezwaar tegen het voorstel van wet en adviseert u dit niet in te dienen.

Openbaarmaking

Aangezien het wetsvoorstel in openbare consultatie is gegeven, is het CBP voornemens het onderhavige wetgevingsadvies op of na 12 februari 2015 openbaar te maken.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Lid van het College

DATUM 10 februari 2015

ONS KENMERK

Bijlage bij de brief van het College bescherming persoonsgegevens van 10 februari 2015 inzake het conceptwetsvoorstel Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische communicatiediensten

1. Inhoud van het wetsvoorstel

Artikel I van het wetsvoorstel betreft een wijziging van de Telecommunicatiewet. Hierin wordt vastgelegd dat telecomaanbieders verplicht zijn de door de aangepaste Wet bewaarplicht telecommunicatiegegevens vereiste gegevens gedurende zes dan wel twaalf maanden te bewaren teneinde te kunnen voldoen aan een vordering door de opsporingsdiensten. Tevens wordt vastgelegd dat de gegevens dienen te worden opgeslagen en verwerkt in Nederland, of in elk geval in een van de lidstaten van de Europese Unie.

Artikel I, onderdeel E biedt het Agentschap Telecom in de toekomst de mogelijkheid de gegevens inhoudelijk te controleren, onder meer om te kunnen nagaan of aan de verwijderplicht is voldaan.

Artikel I, onderdeel F bevat een wijziging van de bijlage bij artikel 13.2a van de Telecommunicatiewet, waarin de lijst met gegevens die dient te worden bewaard is vastgelegd. Er wordt een aantal te bewaren gegevens geschrapt uit de lijst (waaronder MMS en het gebruik van e-mail over internet). Daarnaast wordt de bewaarplicht voor Voice-over-IP telefoondiensten over een vast of mobiel netwerk verruimd van zes naar twaalf maanden. Ten slotte wordt de omschrijving van de bij het IP-adres te bewaren gegevens aangepast en wordt vastgelegd dat het last Cell ID (locatiegegeven afgeleid van de mast bij het beëindigen van een gesprek) niet hoeft te worden bewaard.

Artikel II van het wetsvoorstel behelst een aanpassing van de aan de bewaarplicht gelieerde bepalingen uit het Wetboek van Strafvordering. Een vordering van de gegevens door de officier van justitie wordt volgens deze bepalingen afhankelijk gemaakt van voorafgaande machtiging door de rechter-commissaris. De toegang tot de bewaarde telefoniegegevens (inclusief Voice-over-IP over vaste of mobiele netwerken) wordt gedifferentieerd, afhankelijk van de aard van het misdrijf. In beginsel geldt een termijn van zes maanden; alleen bij de opsporing en vervolging van strafbare feiten waarop een vrijheidsstraf van acht jaar is gesteld, mogen de gegevens die gedurende de volledige bewaartermijn zijn vastgelegd, worden gevorderd. Ten aanzien van internetgegevens wordt geen onderscheid aangebracht.

2. Beoordeling van het wetsvoorstel

2.1 Noodzakelijkheid van een algemene bewaarplicht van 6-12 maanden

In het arrest van 8 april 2014 heeft het Hof van Justitie van de Europese Unie (hierna: het Hof) geoordeeld dat de bewaarplicht, zoals deze destijds is vastgesteld door de Europese wetgever, in strijd is met artikel 7 en 8 van het Handvest.

De Nederlandse bewaarplicht is niet alleen ingevoerd op basis van de Richtlijn dataretentie, maar ook op de voet van artikel 15(1) van de ePrivacy Richtlijn. Dit biedt lidstaten de mogelijkheid nationale bewaarplichten in te voeren in het belang van de staatsveiligheid en voor het voorkomen, opsporen en vervolgen van strafbare feiten, mits deze wetgeving een noodzakelijke, passende en proportionele maatregel is in een democratische samenleving. De richtlijn schrijft voor dat dergelijke maatregelen moeten voldoen aan de algemene beginselen van het gemeenschapsrecht, inclusief het bepaalde in artikelen 6(1) en (2) van het Europees Verdrag, waaruit naleving van artikel 8 EVRM volgt. Nadien is het Handvest aangenomen. Op grond van artikel 51 van het Handvest is het Handvest ook van toepassing op nationale handelingen binnen het toepassingsgebied van het recht van de Unie. Daarom dient de nationale wetgeving te voldoen aan het bepaalde in artikel 7 en 8 van het Handvest. Dit wordt door de regering ook erkend in de beleidsbrief aan de Kamer[1] en in de Memorie van Toelichting bevestigd.[2]

Het Hof schrijft dat op grond van artikel 52 van het Handvest beperkingen kunnen worden gesteld aan de rechten op de persoonlijke levenssfeer en de bescherming van persoonsgegevens, zoals vastgelegd in artikel 7 en 8 van het Handvest. Dit kan echter alleen, wanneer deze beperkingen *"noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden"*.[3] Het Hof overweegt dat het materiële doel van de dataretentierichtlijn – het onderzoek, de opsporing en de vervolging van ernstige criminaliteit – gezien kan worden als een doel van algemeen belang, omdat deze gegevens in de woorden van de Raad justitie en binnenlandse zaken van 19 december 2002 *"een waardevol instrument vormen bij het voorkomen van strafbare feiten en het bestrijden van criminaliteit, met name van de georganiseerde misdaad."*[4] Daarmee stelt het Hof vast dat het gebruik van telecommunicatiegegevens door politie en justitie als zodanig niet strijdig is met het Handvest. Op het punt van de noodzaak van het bewaren van de telecommunicatiegegevens voor de strijd tegen de georganiseerde criminaliteit schrijft het Hof in het arrest dat het *"weliswaar van primordiaal belang is om de openbare veiligheid te waarborgen"*, maar dat *"een dergelijke doelstelling van*

---

[1] Bijlage Reactie van het Kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie van 17 november 2014 (hierna: Beleidsbrief Kabinet) bij *Kamerstukken II* 2013/14, 33542, nr. 16, 27 november 2014, p. 7-8

[2] *Kamerstukken II* 2013/14, 33542, nr. 16, 27 november 2014 (hierna: Memorie van Toelichting), p. 7: *"Toetsing van de Wet bewaarplicht telecommunicatiegegevens aan het Handvest leidt tot de conclusie dat deze wet moet worden aangepast."*

[3] Hofarrest, paragraaf 38.

[4] Hofarrest, paragraaf 43.

algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd."[5]

De regering stelt in haar beleidsbrief over de bewaarplicht overtuigd te zijn *"van het belang en de onmisbaarheid van een bewaarplicht voor telecommunicatiegegevens. Met een bewaarplicht wordt zeker gesteld dat bepaalde telecommunicatiegegevens beschikbaar zijn voor de opsporing en vervolging van ernstige strafbare feiten."*[6] Volgens de regering is de *essentie van de bewaarplicht (...). dat bepaalde telecommunicatiegegevens beschikbaar moeten zijn voor de opsporing van ernstige misdrijven. Als de gegevens voor dat doel strikt noodzakelijk zijn, dan is bewaring daarvan aan de orde ."*[7] In de Memorie van Toelichting schrijft de regering: *"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."*[8]

Enkel het algemeen belang van de beschikbaarheid van telecommunicatiegegevens voor de opsporing rechtvaardigt op zich nog niet de noodzaak voor een algemene bewaarplicht van 6 tot 12 maanden. De regering lijkt in de beleidsbrief een doelredenering te gebruiken: als bepaalde gegevens noodzakelijk zijn voor de opsporing, dan is een algemene bewaarplicht noodzakelijk.

Het CBP constateert dat de feitelijke onderbouwing in het wetsontwerp van de noodzaak om deze gegevens van *de facto* elke Nederlander gedurende zes tot twaalf maanden te bewaren, tekort schiet. Zowel ten tijde van de invoering van de Wet bewaarplicht telecommunicatiegegevens[9], als nu bij de voorgestelde aanpassing ervan, gebruikt de regering voor de onderbouwing van de noodzaak van deze bewaarplicht kwalitatief onderzoek van respectievelijk de Erasmus Universiteit[10] en het WODC.[11] Deze rapporten geven de opvattingen weer van de ondervraagde experts uit de opsporingspraktijk, samengevat inhoudende dat de gegevens onmisbaar zijn voor de opsporing. Beide rapporten geven aan dat het niet mogelijk is om kwantitatief onderzoek te verrichten naar de relatie tussen het aantal opgevraagde historische telecommunicatiegegevens en de effectiviteit hiervan bij de bestrijding van ernstige misdrijven.[12]

---

[5] Hofarrest, paragraaf 51.

[6] Beleidsbrief Kabinet, p. 6.

[7] Idem, p. 10.

[8] Memorie van Toelichting, p. 10.

[9] De Wet bewaarplicht telecommunicatiegegevens is op 1 september 2009 in werking getreden.

[10] P. A.M. Mevis e.a., 'Wie wat bewaart heeft wat: Onderzoek naar nut en noodzaak van een bewaarverplichting van historische verkeersgegevens van telecommunicatie'. Erasmus Universiteit Rotterdam, 2005, URL: https://www.eerstekamer.nl/eu/behandeling/20050616/rapport_bijlage_bij_brief_5357934 (hierna: Mevis rapport).

[11] G. Odinot, D. de Jong, R.J. Bokhorst, C.J. de Poot, 'De Wet bewaarplicht telecommunicatiegegevens, Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing'. WODC 310, 2013, URL: https://www.wodc.nl/images/ob310-volledige-tekst_tcm44-534136.pdf (hierna: WODC rapport).

[12] WODC rapport, p. 29: *"Het is echter niet mogelijk om – zoals bij een product- of effectevaluatie het geval is – het effect vast te stellen van de invoering van de Wet bewaarplicht op de wijze waarop verkeersgegevens gebruikt worden in de opsporingspraktijk. Dit is niet goed mogelijk omdat de telecommunicatiegegevens waar het hier om draait ook vóór de*

Hoewel de bewaarplicht sinds 1 september 2009 in werking is getreden, en de opsporingsautoriteiten ruim vier en half jaar ervaring hebben opgedaan, is het kennelijk niet mogelijk gebleken een systematische onderbouwing te leveren van de noodzaak van deze bewaarplicht. Het CBP merkt tegelijkertijd op dat in Nederland veel gebruik wordt gemaakt van de bevoegdheid om bewaarde internet en telefoniegegevens op te vragen. In 2012 werden 56.825 vorderingen voor telecommunicatiegegevens gedaan door Justitie. Van dit totaal hadden volgens WODC 41.658 vorderingen betrekking op gegevens die in het kader van de bewaarplicht werden bewaard. Bijna de helft (42,6%) van deze vorderingen betrof gegevens die niet ouder waren dan drie maanden.[13] Ten aanzien van mastgegevens was zelfs 79% van de gevraagde gegevens niet ouder dan drie maanden.[14] De onderzoekers concluderen dat in driekwart van de gevallen de gevraagde gegevens niet ouder waren dan maximaal een half jaar.[15] Tegenover dit hoge aantal bevragingen staan 74 strafuitspraken van rechtbanken en hoven die de onderzoekers hebben gevonden waarin historische verkeersgegevens in dat jaar kenbaar een rol speelden.[16]

In dit overzicht van rechtszaken is geen nader onderscheid gemaakt tussen gegevens die beschikbaar zouden zijn geweest in de systemen van de telecomaanbieders zonder dat er een bewaarplicht was ingevoerd, of gegevens die bij aanvang van een onderzoek 'bevroren' hadden kunnen worden door de aanbieders, ten behoeve van later onderzoek. Uit het WODC-rapport blijkt dat het zwaartepunt van het opvragen van verkeersgegevens ligt bij het begin van het onderzoek.[17] Het wetsvoorstel bevat in het geheel geen uitwerking van de subsidiariteitstoets en onderbouwt niet waarom het alternatief van bevriezing van telecommunicatiegegevens, waarbij een relatie gelegd kan worden met ernstige criminaliteit, geen werkbaar alternatief oplevert ten

---

invoering van de Wet bewaarplicht in het algemeen beschikbaar waren voor de opsporing en gebruikt werden in de opsporingspraktijk." en Mevis rapport, p. 6: "*Het feit dat er uit de aangeboden selectie 65 zaaksdossiers zijn gevonden waarbinnen het gebruik van historische verkeersgegevens een (belangrijke) rol heeft gespeeld, kan niet leiden tot de wetenschappelijk onderbouwde conclusie dat die gegevens dus van (essentieel) belang zijn voor alle opsporingsonderzoeken. Uit de gehouden interviews kwam wel duidelijk naar voren dat men binnen de opsporing met grote regelmaat gebruik maakt van onderhavige bevoegdheid en dat veel voor de opsporing relevante informatie door middel van deze bevoegdheid verzameld wordt.*" In het Mevis rapport wordt ook de volgende conclusie getrokken: "*Wil men wetenschappelijk onderbouwde conclusies trekken over nut en noodzaak binnen de opsporingspraktijk van een bewaartermijn ruimer dan de nu gebruikelijke drie maanden, zou er zicht moeten zijn op het aantal strafrechtelijke onderzoeken die voordeel gehad zouden hebben bij een ruimere bewaartermijn en dus niet opgelost zijn of een langere doorlooptijd hebben gehad vanwege het niet meer aanwezig zijn van historische verkeersgegevens bij de aanbieders. In de aangeleverde opsporingsonderzoeken zijn dergelijke dossiers niet aangetroffen.*" Idem.

[13] WODC rapport, p. 120.

[14] WODC rapport, p. 121.

[15] WODC rapport, p. 87, tabel 6.1.1.

[16] Van de in totaal gepubliceerde en door het WODC geselecteerde 2.990 gepubliceerde strafuitspraken, kwamen historische verkeersgegevens voor in 74 uitspraken. WODC rapport, p. 128-129. Dit betreft dus minder dan een kwart procent van de gevallen. Ten aanzien van het gebruik van IP-adressen hebben de onderzoekers, zelfs met een langere zoekperiode van vier jaar, slechts 26 strafuitspraken gevonden. WODC rapport, p. 138.

[17] WODC rapport, p. 85.

opzichte van een algemene bewaarplicht. Een dergelijke specifieke bewaarplicht zou in zijn aard een geringere inbreuk maken op de rechten van alle Nederlanders.

Zonder afbreuk te willen doen aan de ernst van de voorbeelden die de regering in de Memorie van Toelichting geeft van het belang van het gebruik van historische telecommunicatiegegevens bij de opsporing van bepaalde vormen van ernstige criminaliteit, betreft het geen systematisch, met het gewicht van de voorgestelde maatregel overeenkomend, betoog over de noodzaak van de algemene bewaarplicht. De gegeven voorbeelden zijn, als het om het bewaren van internetverkeersgegevens gaat, eerder contrair aan het betoog dat een bewaartermijn van zes maanden noodzakelijk is voor de bestrijding van genoemde zeer ernstige misdrijven. In beide internetvoorbeelden gaat het over internetgegevens die pas na zes maanden of langer werden opgevraagd, en dus niet beschikbaar zouden zijn onder de bewaarplicht telecommunicatiegegevens.

Het CBP concludeert samenvattend dat het wetsontwerp geen adequate onderbouwing biedt van de noodzaak voor een algemene bewaarplicht voor internet en (internet)telefoniegegevens gedurende zes, respectievelijk twaalf maanden.

Ten aanzien van het noodzakelijkheidsvereiste wijst het CBP voorts op de jurisprudentie van het Europees Hof van de Rechten van de Mens (hierna: EHRM) ten aanzien van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM). Het EHRM heeft bij herhaling[18] gesteld dat een inperking van een grondrecht gerechtvaardigd kan zijn, wanneer dit in lijn is met nationale wetgeving, een rechtmatig doel wordt nagestreefd en de noodzaak in een democratische samenleving kan worden aangetoond. Er is echter geen vrijbrief voor landen om elke maatregel die passend wordt geacht ook in te voeren, aldus het EHRM in Klass/Duitsland: "*The Court, being aware of the danger such a law* [wetgeving die geheime surveillance mogelijk maakte, samenvatting CBP] *poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*"[19]

2.2 *Proportionaliteit van een algemene bewaarplicht (van alle personen)*

In het Hofarrest wordt veel aandacht besteed aan de proportionaliteitstoets, dat wil zeggen, de evenredigheid van het gekozen middel ten opzichte van het ermee te bereiken doel, in relatie tot de inbreuk die ermee wordt gemaakt op de grondrechten van burgers.

Het Hof stelt allereerst vast dat de dataretentierichtlijn van toepassing is "*op alle personen, alle elektronische communicatiemiddelen en alle telecommunicatiegegevens, zonder dat enig onderscheid wordt*

[18] Zie onder meer Leander/Zweden (EHRM, 26 maart 1987), paragrafen 49-67; K & T/Finland (EHRM, 12 juli 2001), paragrafen 151-155, S. en Marper/Verenigd Koninkrijk (EHRM, 4 december 2008), paragrafgen 95-104 en Khelili/Zwitserland (EHRM, 18 oktober 2011), paragrafen 58-71.

[19] Klass e.a./Bondsrepubliek Duitsland (EHRM 6 september 1978), paragraaf 49.

gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel, zware criminaliteit te bestrijden."[20] Ook stelt het Hof vast dat de richtlijn geen expliciete regeling biedt voor de toegang tot de gegevens. (Op dit punt voorziet het wetsvoorstel in een aanpassing.) Het Hof concludeert op basis van beide argumenten dat de dataretentierichtlijn *"geen duidelijke en precieze regels bevat betreffende de omvang van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten. Vastgesteld moet dus worden dat deze richtlijn een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke."*[21]

De analyse van het Hof komt in grote lijnen overeen met de kritiek die sinds de eerste voorstellen voor een bewaarplicht is geuit door de Europese toezichthouders voor gegevensbescherming, verenigd in de Artikel 29 Werkgroep. In een verklaring uit 2002, toen via de ePrivacy richtlijn de mogelijkheid van een nationale bewaarplicht telecommunicatiegegevens werd ingevoerd, schreven de toezichthouders: *"The European Data Protection Commissioners have grave doubt as to the legitimacy and legality of such broad measures. (...) The European Data Protection Commissioners have repeatedly emphasized that such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention of Human Rights (...)."*[22]

De Artikel 29 Werkgroep heeft deze beoordeling nadien verscheidene malen herhaald. In het najaar van 2005 stelde de Artikel 29 Werkgroep onder meer: *"A proportionate balance must be struck to ensure that we do not undermine the kind of society we are seeking to protect. This balance is especially necessary when forcing communication service providers to store data that they themselves have no need for. In this manner, one could eventually achieve the unprecedented, continued, pervasive monitoring of all kinds of communication and movement of the totality of citizens in their daily life. A huge amount of information would be stored that is actually useful for investigational purposes in a limited number of cases."*[23]

De zorg over de proportionaliteit wordt in het Hofarrest als volgt verwoordt: : *"Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt (...) bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden."*[24]

---

[20] Hofarrest, paragraaf 57-58.

[21] Hofarrest, paragraaf 65.

[22] Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 september 2002) on mandatory systematic retention of telecommunications traffic data, door het CBP bij brief van 2 september 2002 aangeboden aan de Minister van Justitie, CBP z2002-0885.

[23] Artikel 29-werkgroep, Opinie 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), 21 oktober 2005, p. 5.

[24] Hofarrest, paragraaf 37.

Het feit dat de bewaarplicht ziet op gegevens over het telecommunicatieverkeer, en niet op de inhoud van gesprekken, e-mails of websurfgedrag, maakt niet dat sprake is van een geringe inbreuk op het grondrecht bescherming persoonsgegevens. In 1984 heeft het EHRM al geoordeeld dat verkeersgegevens een integraal element vormen van de telecommunicatie, en dat het verstrekken van deze gegevens aan de politie een inbreuk vormt op het recht op privacy.[25]

De Artikel 29 Werkgroep schrijft hierover in zijn opinie naar aanleiding van de Snowden-onthullingen: *"It is also particularly important to note that metadata often yield information more easily than the actual contents of our communications do. They are easy to aggregate and analyse because of their structured nature. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours. This is not the case for the conversations, which can take place in any form or language. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours."*[26]

Verkeersgegevens zijn daarom persoonsgegevens, die net zoveel bescherming behoeven als de inhoud van communicatie tussen personen.[27, 28, 29] Op grond van het wetsontwerp dienen de

---

[25] Malone/Verenigd Koninkrijk (EHRM, 2 augustus 1984), paragraaf 84. Het verwerken van verkeersgegevens *"is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts [...] to an interference with a right guaranteed by Article 8."*

[26] Artikel 29-Werkgroep, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 april 2014, p. 5. De Werkgroep onderbouwt dit standpunt onder meer met een verwijzing naar de schriftelijke verklaring die professor E.W. Felten heeft afgelegd ten overstaan van de United States District Court for the Southern District of New York in de zaak ACLU v. Clapper.

[27] Zie ook het rapport van de VN Hoge Commissaris voor de Mensenrechten, The right to privacy in the digital age, 30 juni 2014, URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/ Session27/ Documents/A.HRC.27.37_en.pdf, paragrafen 19-20: *"The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. As the European Union Court of Justice recently observed, communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained." (...) It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful* [onderstreping toegevoegd door het CBP]." En paragraaf 26: "*Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.*"

[28] Zie ook de mede door Nederland ingediende resolutie van 19 november 2014 van het Derde Comité van de Algemene Vergadering van de Verenigde Naties over The Right to Privacy in the Digital Age, URL:

telecommunicatieaanbieders deze gegevens van alle klanten te bewaren, ook de gegevens van klanten waarbij in het geheel geen aanwijzingen bestaat dat hun gedrag verband houdt met zware criminaliteit of dat er een verband bestaat met bedreiging van de openbare veiligheid.

In de beleidsbrief aan de Kamer schrijft de minister: "*Als de gegevens van deze personen niet bewaard mogen worden voordat het strafbare feit is gepleegd, zou het stellen van een dergelijke zoekvraag niet zinvol zijn. Het bewaren van bepaalde gegevens van alle burgers is derhalve noodzakelijk, nu niet op voorhand bij de opslag al kan worden onderscheiden tussen verdachte en niet-verdachte burgers.*"[30]

In deze beleidsbrief staat ook: "*Met het vereiste dat op basis van objectieve criteria per categorie gegevens duidelijk en precies wordt omschreven voor welke periode het strikt noodzakelijk is dat de gegevens door telecommunicatieaanbieders moeten worden bewaard, wordt voorbij gegaan aan de essentie van de bewaarplicht. Deze is dat bepaalde telecommunicatiegegevens beschikbaar moeten zijn voor de opsporing van ernstige misdrijven. Als de gegevens voor dat doel strikt noodzakelijk zijn, dan is bewaring daarvan aan de orde.*"[31]

Het feit dat de bewaarplicht niet wordt ingekaderd, en volgens de regering ook niet kán worden ingekaderd tot enkel die gegevens die noodzakelijk zijn om het beoogde doel te bereiken – de bestrijding van zware criminaliteit –, maakt dat de inbreuk op de artikelen 7 en 8 van het Handvest te groot is, en dat de maatregel niet voldoet aan het proportionaliteitsvereiste van artikel 8 EVRM. Naar het oordeel van het CBP kan hieruit worden afgeleid dat de voorgestelde instandhouding van een algemene bewaarplicht strijdig is met de in Europa geldende grondrechten, tenzij aan dit bewaren van de gegevens vooraf beperkingen kunnen worden gesteld.

Het CBP gaat in paragraaf 2.3 van dit advies nader in op het onderscheid dat de regering voorstelt tussen het bewaren van gegevens en de toegang ertoe, maar constateert hier reeds dat onder meer de conclusies van het Hof nopen tot heroverweging van het uitgangspunt van een algemene bewaarplicht voor telecommunicatiegegevens van *de facto* iedere Nederlander en daarmee van het gehele wetsontwerp.

Voor het CBP weegt het gebrek aan specifieke afbakening bij de evenredigheidstoets het zwaarst. Dit laat onverlet dat het wetsvoorstel, ook bij een eventueel nader afgebakende bewaarplicht, nog aan drie andere voorwaarden dient te voldoen om de proportionaliteitstoets te doorstaan. Dit zijn:

1. naleving van de notificatieplicht;

---

http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/69/L.26/Rev.1

"Noting that while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity."

[29] Zie ook CBP advies van 11 februari 2013 over het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet (z2012-00746), p. 5-7.

[30] Beleidsbrief Kabinet, p. 8.

[31] Idem, p. 10.

2. controle op het gebruik van de bewaarde gegevens;
3. uitzonderingen voor mensen met een beroepsgeheim.

2.2.1 Naleving van de notificatieplicht

Het CBP leest in het Hofarrest een aanwijzing dat notificatie aan betrokkenen dat hun telecommunicatiegegevens zijn opgevraagd, een bijdrage levert aan de proportionaliteit van een maatregel om (specifieke) gegevens te bewaren ten behoeve van de opsporing. Zonder een deugdelijk notificatiesysteem kan bij iedereen in Nederland het gevoel ontstaan dat zij voortdurend bespied worden. Het Hof schrijft: "*Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of de geregistreerde gebruiker hierover wordt ingelicht, bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden, zoals de advocaat-generaal in de punten 52 en 72 van zijn conclusie heeft opgemerkt* [onderstreping toegevoegd door het CBP]."[32] Het CBP vraagt zich af hoe deze constatering van het Hof zich verhoudt tot de voorgenomen afschaffing van de notificatieplicht, zoals voorgesteld bij wetsontwerp van 30 september 2013.[33] Op 25 november 2013 heeft de vaste commissie voor Veiligheid en Justitie verslag uitgebracht; sindsdien heeft de minister niet meer gereageerd.

2.2.2 Controle op het gebruik van de bewaarde gegevens

In het gewijzigde artikel 13.9 van de Telecommunicatiewet is sprake van 'een verslag over de doeltreffendheid en de effecten van deze wet in de praktijk', dat elke drie jaar na de inwerkingtreding aan de Staten-Generaal wordt toegezonden. Van een horizonbepaling is geen sprake, evenmin als van een concrete invulling van de minimumvereisten waaraan een dergelijk verslag zou moeten voldoen.

Het CBP heeft kennis genomen van initiatieven van marktpartijen om anonieme en geaggregeerde statistieken openbaar te maken over aantallen intercepties en bevragingen van verkeers- en gebruikersgegevens. Hun doel is maatschappelijke transparantie te verschaffen over het gebruik van deze ingrijpende bevoegdheden door de overheid. De Minister van Veiligheid en Justitie heeft de telecom- en internetaanbieders, in beantwoording van Kamervragen hierover, ernstig ontraden om dergelijke statistieken openbaar te maken.[34] De minister verwijst daarbij naar een eerdere uitspraak van de staatssecretaris "*dat de verstrekking van geaggregeerde informatie de belangen van opsporing en vervolging ernstig in de weg kan staan. Een dergelijke verstrekking kan namelijk inzicht geven in de werkwijzen van de politie en het openbaar ministerie en kwaadwillenden zouden op basis hiervan hun werkwijze kunnen aanpassen.*"

---

[32] Hofarrest, paragraaf 37.

[33] *Kamerstukken II*, 2013/14, 33 747, Wijziging van het Wetboek van Strafvordering en het Wetboek van Burgerlijke Rechtsvordering in verband met de versterking van het presterend vermogen van de politie.

[34] *Aanhangsel Handelingen*, 2013/14, 2014Z01266, 24 maart 2014.

De minister neemt in het jaaroverzicht van het ministerie van Veiligheid en Justitie een overzicht op van het totale aantal vorderingen 'historische gegevens' door het OM.[35] Dit jaarlijkse totaalaantal biedt echter geen inzage in de bevragingen door inlichtingen- en veiligheidsdiensten, en is bovendien moeilijk te interpreteren, omdat niet gespecificeerd is om hoeveel personen het gaat, over welke termijnen het gaat, en om wat voor soorten criminaliteit. WODC schrijft hierover: (...) *het opvragen van telecomgegevens in Nederland wordt geregistreerd per telefoonnummer, IMEI-nummer, IP-adres of 'paallocatie', waarover gegevens worden opgevraagd. Omdat mensen vaak meerdere telefoons gebruiken, geven deze cijfers geen inzicht in het aantal personen van wie er jaarlijks telecomgegevens worden opgevraagd of van het aantal opsporingsonderzoeken of de aard van de opsporingsonderzoeken waarvoor deze gegevens worden opgevraagd."*[36] Ook bij het vorderen van mastgegevens gaat het om meer betrokken personen, omdat dan informatie wordt verkregen over alle mobiele gesprekken die op een bepaald tijdstip via een bepaalde mast zijn gevoerd. Bovendien betreffen de statistieken ook vorderingen van gegevens die niet onder de Wet bewaarplicht vallen.[37]

De stelling dat personen hun werkwijze zouden kunnen aanpassen op grond van anonieme, geaggregeerde statistieken, is niet onderbouwd. De regering gaat zonder toelichting voorbij aan het advies van het WODC om meer inzicht te bieden *"door de vorderingen zodanig te registreren dat zichtbaar wordt over hoeveel personen er jaarlijks telecommunicatieverkeersgegevens worden opgevraagd, in hoeveel zaken dit gebeurt en voor welke soort zaken deze gegevens worden opgevraagd."*[38] Het ontbreken van transparantie op dit punt staat democratische controle op de (effectiviteit van de) uitoefening van bevoegdheden in de weg, en biedt ook geen inzicht aan burgers over de inzet van dit instrument.[39]

2.2.3 Uitzonderingen voor mensen met een beroepsgeheim

Aanvullend merkt het CBP op dat de voorgestelde wetsaanpassing niet tegemoet komt aan een ander kritiekpunt van het Hof, te weten dat de richtlijn geen uitzonderingen bevat voor de communicatie van mensen met een beroepsgeheim, zoals artsen, advocaten, notarissen of journalisten.[40]

---

[35] *Kamerstukken II*, 2013–2014, 33 930 VI, nr. 1, p. 50. Het meest recente jaarverslag bevat cijfers over 2013. In dat jaar zijn 62.554 ' aanvragen op historische gegevens' door het OM gedaan. Dit aantal omvat volgens de voetnoot zowel verkeersgegevens als identificerende gegevens.

[36] WODC rapport, p. 119.

[37] WODC rapport, p. 120.

[38] WODC rapport, p. 124.

[39] Het CBP wijst op het EHRM-arrest Youth Initiative For Human Rights/Servië (EHRM, 25 juni 2013), paragrafen 25-26. Ook de VN Hoge Commissaris voor de Mensenrechten merkt op: *"A second and related observation concerns the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability."* (paragraaf 48).

[40] Hofarrest, paragraaf 58: *"Bovendien bevat de richtlijn geen uitzonderingen, zodat zij zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het zakengeheim vallen."*

Samenvattend oordeelt het CBP dat de voorgestelde aanpassingen van de Wet bewaarplicht niet door de noodzakelijkheids-, proportionaliteits- en subsidiariteitstoets komen, en dat het wetsvoorstel op drie specifieke punten in strijd blijft met het proportionaliteitsvereiste, zoals vastgelegd in de artikelen 7 en 8 van het Handvest en in artikel 8 van het EVRM.

2.3 *Verzamelen versus het gebruiken van gegevens*

De regering stelt voor om een onderscheid te maken tussen het bewaren van de gegevens, en het gebruik ervan door de opsporings- en inlichtingendiensten en beschrijft dit in de beleidsbrief als een belangrijke waarborg om de inbreuk op de persoonlijke levenssfeer van betrokkenen te matigen. De regering stelt in de beleidsbrief dat de overwegingen van het Hof in samenhang dienen te worden bezien. De inbreuk die door de bewaarplicht telecommunicatiegegevens wordt gemaakt op de fundamentele rechten van burgers dient mede te worden vastgesteld aan de hand van de wettelijke waarborgen waarmee de bewaarplicht wordt omkleed. De regering meent zich in dit standpunt gesteund door overweging 69 van het arrest, waarin het Hof zijn conclusie trekt "gelet op een en ander" (*"having regard to all the foregoing considerations"*). Hieruit kan inderdaad opgemaakt worden dat de kritiek van het Hof in samenhang dient te worden bezien en dat het aanpassen van een onderdeel tot een andere conclusie zou kunnen leiden over het geheel.

Het CBP onderschrijft dat er een zekere samenhang bestaat tussen de mate van inbreuk en de voorziene waarborgen. Deze waarborgen dienen echter te gelden voor alle vormen van gegevensverwerking, waaronder in elk geval begrepen bewaren en het gebruik van de gegevens.

Het gaat hierbij niet om de gerichte opslag van gegevens van burgers die verdacht worden van misdrijven, maar om de ongerichte opslag van telecommunicatiegegevens over alle burgers. Of, zoals het Hof schrijft: (de richtlijn is van toepassing) "*op alle personen die gebruikmaken van elektronische communicatiediensten, zonder dat de personen van wie de gegevens worden bewaard zich echter, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met zware criminaliteit.*"[41]

Over de inbreuk die deze algemene bewaarplicht van persoonsgegevens vormt, schrijft de regering in de beleidsbrief: "*Ook de jurisprudentie van het EHRM geeft geen steun aan de opvatting dat een dergelijke gegevensopslag niet is toegestaan.*"[42] De zin is niet voorzien van een voetnoot met verwijzing naar de bedoelde jurisprudentie, en ook in de Memorie van Toelichting wordt hieraan geen aandacht besteed. In zijn arrest verwijst het Hof specifiek naar artikel 8 EVRM en de zaken Liberty e.a./Verenigd Koninkrijk, Rotaru/Roemenië, S. en Marper/Verenigd Koninkrijk en M. K./Frankrijk.[43]

---

[41] Hofarrest, paragraaf 58.

[42] Beleidsbrief Kabinet, p. 9.

[43] Hofarrest, paragrafen 47, 54 en 55.

In het S. en Marper/Verenigd Koninkrijk-arrest uit 2008 concludeerde het EHRM juist dat de opslag van (DNA- en vingerafdruk-)gegevens een inbreuk op de bescherming van de persoonlijke levenssfeer vormde, onafhankelijk van eventueel verder gebruik van die gegevens:

"The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see Leander v. Sweden, 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (see Amann v. Switzerland [GC], no. 27798/95, § 69, ECHR 2000-II)."[44]

In vergelijkbare woorden liet het Hof zich uit in het Liberty e.a./Verenigd Koninkrijk arrest:
"The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (see Weber and Saravia, cited above, § 78)."[45]

In het arrest Rotaru/Roemenië kwam het Hof acht jaar daarvoor al tot dezelfde conclusie: *"The Court points out that both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention (see the following judgments: Leander cited above, p. 22, § 48; Kopp v. Switzerland, 25 March 1998, Reports 1998-II, p. 540, § 53; and Amann cited above, §§ 69 and 80)."*[46]

In het meeste recente door het Hof geciteerde arrest, M. K./Frankrijk (2013), over de opslag van vingerafdrukken, geeft het Hof aan dat de toegang tot de bewaarde gegevens voldoende goed gedefinieerd en afgebakend is, maar dat dat van de verzameling en de opslag niet gezegd kan worden. Het Hof wijst het argument van de Franse regering dat de vingerafdrukken ook gebruikt kunnen worden om iemands onschuld te bewijzen in heldere bewoordingen af:
"Besides the fact that such a reason is not explicitly mentioned in the provisions of Article 1 of the impugned decree, barring a particularly extensive interpretation of this Article, the Court considers that accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant" [onderstreping toegevoegd door het CBP].[47]

Het CBP wijst in dit verband ook op de factsheet van het EHRM over de jurisprudentie met betrekking tot gegevensbescherming. De eerste alinea van dit overzicht is gewijd aan de vaststelling dat louter het opslaan van gegevens over iemands privéleven een inbreuk vormt op

---

[44] S. en Marper/Verenigd Koninkrijk (EHRM, 4 december 2008), paragraaf 67.

[45] Liberty e.a./Verenigd Koninkrijk (EHRM, 1 juli 2008), paragraaf 56.

[46] Rotaru/Roemenië (EHRM, 4 mei 2000), paragraaf 46.

[47] M. K./Frankrijk (EHRM, 18 april 2013), paragraaf 37.

artikel 8 EVRM.[48] De inbreuk wordt dus reeds gevormd door het enkele feit dat de gegevens worden opgeslagen (langer dan noodzakelijk voor de bedrijfsvoering) om te voldoen aan de wettelijk vereiste bewaarplicht.

Het CBP concludeert daarom dat het door de regering beoogde onderscheid tussen het bewaren van gegevens en het gebruik ervan, niet leidt tot beëindiging van de geconstateerde onevenredigheid en daarmee onrechtmatigheid van een algemene bewaarplicht verkeersgegevens. In zijn algemeenheid merkt het CBP in dit verband overigens op dat noch in internationale verdragen, noch in de Wet bescherming persoonsgegevens ruimte is te vinden voor het beoogde onderscheid tussen het bewaren van de persoonsgegevens en het gebruiken ervan, zoals het opvragen.

2.4 Overige voorgestelde aanpassingen

De regering komt met het wetsvoorstel tegemoet aan de kritiek van het Hof op het ontbreken van een voldoende afgebakende toegangsregeling in de richtlijn, met name op het ontbreken van het vereiste van onafhankelijke rechterlijke toetsing.[49] In het Wetboek van Strafvordering wordt voorzien in een voorafgaande schriftelijke machtiging door de rechter-commissaris van vorderingen door de officier van justitie. Deze aanpassing geeft het CBP geen aanleiding tot opmerkingen.

Ook komt het wetsvoorstel tegemoet aan de kritiek van het Hof dat de richtlijn niet verplicht stelt dat de gegevens op het grondgebied van de Unie worden bewaard, door aan de Telecommunicatiewet een expliciete verplichting toe te voegen om de gegevens in Nederland of in een andere lidstaat van de Europese Unie op te slaan en te verwerken.

Ten aanzien van het voorgestelde artikel 18.7, tweede lid, van de Telecommunicatiewet merkt het CBP op dat niet alleen het Agentschap Telecom toezicht houdt op het bepaalde bij of krachtens hoofdstuk 13, maar ook het CBP, voor zover het gaat om de verwerking van persoonsgegevens. De zinsnede in de Memorie van toelichting "*Andere toezichthouders (die aldus geen toezicht houden op de zogenoemde bewaarplicht) hebben geen toegang tot deze gegevens*"[50] lijkt het toezicht door het CBP uit te sluiten.

---

[48] EHRM, Press Unit, Factsheet - Data protection (september 2014), "*General Principles. Mere storage of information about an individual's private life amounts to interference within the meaning of Article 8 (right to respect for private life) of the European Convention on Human Rights.*" URL: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[49] Hofarrest, paragraaf 62: "*Maar bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten (...)*"

[50] Memorie van toelichting, p. 24.

Aanvullend merkt het CBP op dat in de richtlijn dataretentie, in artikel 9, tweede lid, was bepaald dat de toezichthoudende instanties "*volledig onafhankelijk zijn bij de uitoefening van de (...) bedoelde taak.*" Daarvan is in het Nederlandse voorstel geen sprake, nu deze taak is toebedeeld aan een agentschap onder directe verantwoordelijkheid van de minister van Economische Zaken. Het Hof benadrukt het belang van onafhankelijk toezicht, zoals vastgelegd in artikel 8, derde lid, van het Handvest. De bewaarde gegevens dienen volgens het Hof om die reden ook op het grondgebied van de Europese Unie te worden bewaard: "*zodat (...) ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest.*" De Memorie van Toelichting onderbouwt niet dat toebedeling van deze toezichtstaak aan een niet-onafhankelijke toezichthouder niet in strijd is met het Handvest en gaat ook niet in op de opmerking die de Raad van State hierover maakt: "*Ten volle moet zijn gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de beveiliging en bescherming van de opgeslagen gegevens.*"[51]

Ten aanzien van de wijzigingen van de lijst te bewaren gegevens merkt het CBP op dat het goed is dat een einde wordt gemaakt aan de onduidelijkheid bij marktpartijen over de omvang van de te bewaren locatiegegevens, nu expliciet is uitgesloten dat ook de locatie van de zendmast bij beëindiging van een gesprek moet worden vastgelegd (last Cell ID). Taalkundig lijken de voorgestelde aanpassingen overigens nog onvoldoende consistent doorgevoerd; er is onder punt B nog steeds sprake van telefonie, terwijl deze gegevens, conform het wetsontwerp, alleen nog op internettoegang zouden moeten zien.

Deze voorgestelde aanpassingen leiden niet tot een ander oordeel van het CBP over de noodzakelijkheid en proportionaliteit van de aangepaste Wet bewaarplicht telecommunicatiegegevens.

---

[51] Advies Raad van State, p. 11. De Raad van State schrijft ook: "(...)*zodat thans niet ten volle wordt gewaarborgd - zoals het Hof verlangt - dat het College bescherming persoonsgegevens toezicht kan houden op de beveiliging en bescherming van de opgeslagen gegevens.*" (p. 12).

0 BD

POLITIE

derdeel Korpsleiding
Korpsstaf

handeld door
Functie
Bezoekadres Juliana van Stolberglaan 4-10
2595 CL Den Haag
Telefoon 088-1699007
E-mail lbestuursondersteuning@knp.politie.nl

Postbus 17107, 2502 CC Den Haag

Ons kenmerk
Uw kenmerk
Datum 18 februari 2015
Bijlage(n)
Pagina 1/2

VERZONDEN 18 FEB. 2015

Aan de Minister van Veiligheid en Justitie
Postbus 20301
2500 EH Den Haag

Onderwerp conceptwetsvoorstel 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 I

Geachte heer Opstelten,

Bij brief van 18 november 2014 heeft u de politie om een reactie gevraagd ten aanzien van het conceptwetsvoorstel 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. Het conceptwetsvoorstel is binnen de politie bestudeerd en besproken. Dit resulteert in de volgende reactie:

Het conceptwetsvoorstel voorziet in een aanpassing van het Wetboek van Strafvordering en de Telecommunicatiewet in het licht van 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 ongeldig verklaard. Het wetsvoorstel voorziet in een bewaarplicht voor bepaald aangewezen telecommunicatiegegevens ten behoeve van de opsporing van ernstige misdrijven, en - ter bescherming en beveiliging van de bewaarde gegevens - in de nodige waarborgen die voortvloeien uit het arrest van het Hof van Justitie.

De voorgestelde aanpassingen rondom de bewaarplicht en de gewijzigde mogelijkheden in de toegang tot te bewaren verkeersgegevens die in het conceptwetsvoorstel zijn opgenomen, zullen bij invoering een aanzienlijke impact hebben op de politieorganisatie en op de opsporing van ernstige misdrijven.

De politie heeft samen met het College van procureurs-generaal een inhoudelijke reactie op het conceptwetsvoorstel voorbereid. Deze reactie is vastgelegd in bijgaande reactiebrief van het College d.d. 13 februari 2015 (kenmerk WBOM/17201) welke dezer dagen bij u wordt ingediend. Ik sluit mij geheel aan bij de inhoudelijke overwegingen van dit advies, en maak ze hiermee mede tot die van ondergetekende.

Hoogachtend,

korpschef

0 BD

NEDERLAND ICT

Ministerie van Veiligheid & Justitie
Directie Wetgeving en Juridische Zaken
t.
Postbus 20301
2500 EH Den Haag

Woerden, 30 januari 2015

Betreft : reactie op consultatie wetsvoorstel dataretentie
Kenmerk : 18 november 2014 / 525682

Veel dank voor de uitnodiging om te reageren op het voorstel voor de 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 (wetvoorstel dataretentie).

Na uitvoerig overleg met de meest betrokken leden van Nederland ICT, hebben wij besloten de reactie op het wetsvoorstel dataretentie aan onze leden zelf te laten. Het is een vraagstuk dat de aanbieders van openbare elektronische communicatiediensten zelf sterk raakt, temeer vanwege de klantrelatie.

Voor toekomstige wetstrajecten houden we ons graag aanbevolen voor een uitnodiging tot reactie.

Met vriendelijke groet,
Nederland ICT

directeur

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@nederlandict.nl
www.nederlandict.nl

ING Bank
IBAN: NL 53 ING B 0662 590546
KvK 30174840

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

de Rechtspraak

Raad voor de rechtspraak

De Minister van Veiligheid en Justitie
mr. I.W. Opstelten
Postbus 20301
2500 EH Den Haag

Afdeling Strategie

bezoekadres
Kneuterdijk 1
2514 EM Den Haag

correspondentieadres
Postbus 90613
2509 LP Den Haag

T (088) 36 10000
F (088) 36 10022
www.rechtspraak.nl

datum 23 februari 2015
contactpersoon
e-mail
telefoonnummer
ons kenmerk
uw kenmerk
onderwerp Advies over het Wetsvoorstel 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
bijlage(n) -

Geachte heer Opstelten,

Bij brief van 18 november 2014, ontvangen op 19 november 2014, met bovengenoemd kenmerk verzocht u de Raad voor de rechtspraak (de "**Raad**") u te adviseren over het Wetsvoorstel 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 (het "**Wetsvoorstel**"). Dit Wetsvoorstel wordt ook wel aangeduid als het Wetsvoorstel Dataretentie.

Het Wetsvoorstel regelt de aanpassing van de Telecommunicatiewet met betrekking tot de bewaring van bepaalde aangewezen telecommunicatiegegevens ten behoeve van het algemene belang van opsporing en vervolging van strafbare feiten. Dit wetsvoorstel voorziet tevens in de nodige waarborgen ter bescherming en beveiliging van de bewaarde gegevens.

Het 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 door een rechter-commissaris.

Na overleg met de gerechten, adviseert de Raad als volgt.[1]

[1] De Raad voor de rechtspraak heeft op grond van artikel 95 van de Wet op de rechterlijke organisatie een wettelijke

Advies
Het Europese Hof van Justitie heeft in zijn uitspraken van 8 april 2014 in de zaken C-293/12 en C-594/12 de Europese dataretentie richtlijn (2006/24/EG), waarop de huidige wetgeving aangaande bewaring en vordering van telecom- en verkeersgegevens is gebaseerd, ongeldig verklaard. Dit heeft geleid tot het onderhavige Wetsvoorstel.

De Raad onderschrijft het belang van dataretentie ten behoeve van de opsporing en vervolging van strafbare feiten. Daarnaast hecht de Raad aan het belang van de bescherming van de persoonlijke levenssfeer van de burger als het de bewaring van diens telecommunicatiegegevens betreft. Dit kan niet anders dan op bij wet voorgeschreven wijze. Uit het oogpunt van de bescherming van grondrechten acht de Raad het wenselijk dat voorafgaande rechterlijke toetsing plaatsvindt. Indien deze rechterlijke toetsing plaatsvindt door de rechter-commissaris zoals het Wetsvoorstel voorstaat, heeft dit aanmerkelijke gevolgen voor de werklast.

Het Wetsvoorstel geeft daarmee aanleiding tot het maken van opmerkingen over de werklast.

Werklastgevolgen
De Raad verwacht dat invoering van het wetsvoorstel gevolgen heeft voor de werklast van de rechtbanken. De Raad verwacht namelijk dat het aantal vorderingen bij de rechter-commissaris structureel toeneemt met ongeveer 42.000 extra vorderingen. Dit zorgt voor extra kosten van ongeveer twee miljoen euro per jaar. Dit wordt hieronder toegelicht.

Door het wetsvoorstel dient de rechter-commissaris alvorens de machtiging te verlenen, iedere vordering van de officier van justitie te beoordelen. De rechter-commissaris neemt in zijn oordeel over de machtiging de verdenking, proportionaliteit, subsidiariteit en de toepassing van het betreffende artikel mee. Het proces-verbaal van de politie is de basis hiervoor. De behandeltijd van een dergelijke vordering is afhankelijk van de omvang van het proces-verbaal en de complexiteit van de zaak. Een proces-verbaal kan uit enkele pagina's bestaan, maar in uitvoerige onderzoeken kan een dergelijk proces-verbaal zeer uitgebreid zijn. De behandeltijd van de extra 42.000 vorderingen wordt daarom geschat op gemiddeld 15 minuten per vordering en gemiddeld 20 minuten per vordering, indien er sprake is van spoed.

De Raad behoudt zich het recht voor om hier op terug te komen, indien na inwerkingtreding van het Wetsvoorstel in de praktijk blijkt dat het om grotere aantallen gaat of gemiddeld meer tijd vergt.

---

adviestaak met betrekking tot nieuwe wets- en beleidsvoorstellen die gevolgen hebben voor de rechtspraak. De adviezen worden vastgesteld na overleg met de gerechten. De Raad voor de rechtspraak is een adviescollege in de zin van artikel 79 en 80 van de Grondwet. Bij het opstellen van zijn adviezen beoordeelt de Raad de voorgenomen wet- en regelgeving in het bijzonder op de gevolgen voor de organisatie en de werklast van de gerechten en op de (praktische) toepasbaarheid en uitvoerbaarheid. Rechters zijn bij de behandeling van individuele zaken niet gebonden aan de inhoud van de wetgevingsadviezen van de Raad voor de rechtspraak.

de Rechtspraak

Raad voor de rechtspraak

Tot slot

Indien na het uitbrengen van dit advies het Wetsvoorstel op belangrijke onderdelen wordt gewijzigd of indien uit nadere uitvoeringsregelgeving belangrijke werklastgevolgen voortvloeien, wordt de Raad graag in de gelegenheid gesteld daarover aanvullend te adviseren. Met het oog op de informatievoorziening aan en de voorbereiding van de gerechten op de invoering van de onderhavige regeling verzoekt de Raad u hem te informeren over de plaatsing van de definitieve tekst van het Wetsvoorstel in het Staatsblad.

Hoogachtend,

.....

Lid Raad voor de rechtspraak

0 BD

Ministerie van Veiligheid en Justitie

Turfmarkt 147

2511 DP Den Haag

Vertrouwelijke versie verstuurd per post, per mail en via internetconsultatie.nl

Betreft: Zienswijze wijziging Telecommunicatiewet en Wetboek van Strafvordering gegevensbewaring

Den Haag, 31 januari 2015

Uw kenmerk

Op 18 november 2014 is het Ministerie van Veiligheid en Justitie een internetconsultatie gestart over het ontwerpvoorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten.

16 December jl. is in het kader van het Platform 13 samenwerkingsverband over de wetswijziging gesproken en aan T-Mobile Netherlands B.V. (hierna: T-Mobile) en de andere aanwezige telecompartijen de consultatie ter hand gesteld met het verzoek om te reageren op het conceptwetsvoorstel. Deze ter hand gestelde consultatie is gebruikt om onderstaande zienswijze op te stellen en daarmee is ook dezelfde paginanummering aangehouden.

T-Mobile dankt het ministerie voor het gesprek op 16 december en voor de mogelijkheid om onze zienswijze te kunnen geven op het conceptwetsvoorstel en maakt graag gebruik van deze gelegenheid.

Op 8 april 2014 heeft het Hof van Justitie van de Europese Unie (hierna: HvJEU) de richtlijn dataretentie ongeldig verklaard. Dit samen met de kabinetsreactie heeft geresulteerd in het wetsvoorstel dat ter consultatie wordt aangeboden.

T-Mobile heeft als grondhouding te voldoen aan datgene wat haar door wetgeving wordt opgelegd, in nauwe samenwerking met overheid en toezichtsorganen. Voor T-Mobile is het van groot belang dat, als het gaat om verkeersgegevens van haar klanten, het voor alle betrokken partijen duidelijk moet zijn welke gegevens bewaard moet worden, onder welke omstandigheden, wanneer en door wie de gegevens opgevraagd en ontsloten mogen worden.

Wetswijziging

Uit het arrest van het HvJEU d.d. 8 april 2014 is duidelijk geworden dat de wet moet worden aangepast op een aantal cruciale onderdelen.

In het conceptwetsvoorstel zijn dan ook een aantal wijzigingen ten opzichte van de vorige wet opgenomen om te voldoen aan de door het HvJEU gestelde vereisten van redelijkheid en proportionaliteit, met als belangrijke aanpassingen de voorafgaande toetsing van de rechter commissaris en de raadplegingstermijnen van 6 of 12 maanden afhankelijk van de hoogte van de gevangenisstraf.

Voorafgaande toetsing

Voor wat betreft het eerste onderdeel, voorafgaande toetsing, wordt dit verwoord in het wetsvoorstel onder artikel 126u lid 4 van het Wetboek van Strafvordering. T-Mobile vraagt zich af op welke wijze een dergelijke rechterlijke toetsing in de praktijk uitgevoerd gaat worden gezien de jaarlijkse hoeveelheid bevragingen. T-Mobile vraagt zich daarbij af of de voorgestelde voorafgaande toetsing een reeel te noemen optie is. Op pagina 18 van het conceptwetsvoorstel onder paragraaf 9 van de Memorie van toelichting wordt door u melding gemaakt van het feit dat deze wijziging gevolgen zal hebben voor het openbaar ministerie en de zittende magistratuur, hieruit lijkt

T-Mobile te kunnen opmaken dat u hiermee aangeeft dat de werkzaamheden door deze voorafgaande toetsing zullen toenemen . T-Mobile vraagt zich hierbij meteen af, als de voorgaande aanname een correcte is, van welke aantallen zal worden uitgegaan.

Op pagina 27 van het conceptwetsvoorstel wordt aangegeven dat artikel 126l lid 7 van het Wetboek van Strafvordering van toepassing is waardoor de machtiging in geval van spoed mondeling gegeven kan worden en dat de machtiging schriftelijk binnen drie dagen wordt gegeven. Afhankelijk van de hoeveelheden mondeling gegeven spoed-machtigingen zal dit voor de aanbieder van telecommunicatie diensten ook tot een toename van administratieve lasten leiden om er onder andere zorg voor te dragen dat T-Mobile op de juiste juridische basis de gegevens heeft verstrekt. De precieze bedrijfseffecten en kosten bespreken wij te zijnertijd graag met u.

Termijnen

De raadplegingstermijnen zijn neergelegd in artikel 126ulid 3 sub a en sub b Wetboek van Strafvordering lijken een stap in de goede richting als die worden afgezet tegen de uitspraak van het HvJEU. Echter in de uitspraak van het Hof wordt gevraagd om de bewaartermijnen te verkorten en op basis van objectieve criteria vast te stellen. In de Memorie van Toelichting worden een aantal gevallen besproken om nut en noodzaak vanuit de opsporing aan te tonen.

De door het Hof gewenste objectieve criteria zien wij echter niet terug. Dit is voor T-Mobile van belang omdat hier mogelijk het Hof niet wordt gevolgd. Wij vragen ons af welke consequenties hieraan kunnen worden verbonden (door zowel de toetsing van de Europese rechter als Nederlandse burgers) en of dit ons als aanbieder van telecommunicatiediensten niet in een juridische en morele spagaat brengt.

Ook het in de Memorie van Toelichting genoemde WODC onderzoek op pagina 9 van de Memorie van Toelichting geeft wat dat betreft weinig houvast om tot objectieve criteria te komen. De bevraagde historische gevens worden voornamelijk gebruikt voor ondersteunend ('sturend') bewijs. Op pagina 12 wordt ook gesproken over weerlegging van bewijs door telecomanalyse. Door een gebrek aan kwantitatieve rapportages over inzet en doelmatigheid van de bevragingen lijkt het ook moeilijk om tot dergelijke criteria te komen. Hierbij dan ook de vraag of het periodiek (jaarlijks) uitvoeren van een dergelijke rapportage ook onderdeel zou kunnen uitmaken van het wetsvoorstel.

Poorten en IPv6

In de Memorie van Toelichting wordt op pagina 25 aangegeven dat er ter identificatie van de gebruiker bij gebruik van Network Adress Translation (NAT) of een vergelijkbare techniek poortnummers moeten worden opgeslagen.

T-Mobile kent op dit moment per device + SIM een routeerbaar (uniek) IP-adres toe. Uit de Memorie van Toelichting zou daarom kunnen worden opgemaakt dat er geen poortnummers hoeven worden opgeslagen. T-Mobile vraagt zich af of dit een juiste aanname is en dat er geen opslag van poortnummers nodig is.

Voor wat betreft de opslag capaciteit voor wat betreft IPv6 wordt er gesproken over een toename van 300% ten opzichte van IPv4. De investering die hiervoor nodig zal zijn is bij ons op dit moment nog niet bekend.

Mocht u over het bovenstaande vragen hebben of een nadere toelichting wensen dan zijn wij altijd bereid tot een persoonlijk gesprek.

Hoogachtend, met vriendelijke groeten,

namens T-Mobile Netherlands B.V.

Sr. Regulatory Affairs Counsel