

College van procureurs-generaal

Voorzitter

Postadres: Postbus 20305, 2500 EH Den Haag.

Minister van Justitie
mr. E.M.H. Hirsch Ballin
Postbus 20301
2500 EH 'S-GRAVENHAGE

Bezoekadres:

Prins Clauslaan 16
2595 AJ Den Haag
Telefoon +31 70 33 99 600
Telefax +31 70 33 99 854

Onderdeel	Bestuurlijke en Juridische zaken
Contactpersoon	mr. C.J. Glorie
Doorkiesnummer(s)	070-3399804
Datum	9 februari 2007
Ons kenmerk	PaG/BJZ-B/11365
Uw kenmerk	545471/06/6
Onderwerp	Advies conceptwetsvoorstel bewaarplicht telecommunicatiegegevens

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

Geachte heer Hirsch Ballin,

Bij brief van 15 november 2006 heeft u het College van procureurs-generaal ter consultatie voorgelegd het concept voor een wetsvoorstel tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van richtlijn 2006/24/EG en tot wijziging van richtlijn 2002/58/EG. In dit wetsvoorstel worden regels gesteld voor de verplichting tot bewaring van gegevens door de aanbieders van openbare telecommunicatiediensten en openbare telecommunicatienetwerken, de bewaartermijn en de bescherming van de door de aanbieders bewaarde gegevens. De bewaarplicht beoogt te garanderen dat de te bewaren gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Het College heeft met belangstelling kennis genomen van het onderhavige voorstel en maakt graag van de gelegenheid gebruik een aantal opmerkingen te maken.

De bewaartermijn

De richtlijn dataretentie legt aan de lidstaten de verplichting op ervoor te zorgen dat de te bewaren gegevens gedurende tenminste zes maanden en ten hoogste twee jaar vanaf de datum van communicatie worden bewaard. Door onderzoekers van de Erasmus Universiteit¹ wordt een bewaartermijn van één jaar aanbevolen. Het College is het zeer eens met uw constatering dat de door de onderzoekers aanbevolen bewaartermijn als een minimum moet worden beschouwd. Het College merkt op dat het rapport van de Erasmus Universiteit zich voor wat betreft de benodigde bewaartermijn voornamelijk richt op het opsporingsonderzoek. In dat kader is het voorstel tot een bewaartermijn van twaalf maanden begrijpelijk. Maar het College wijst er op dat het ook

¹ TK 2004-2005, 23490, nr. 379

tijdens het onderzoek ter terechtzitting noodzakelijk kan zijn te beschikken over de bewaarde gegevens. Bijvoorbeeld als de rechter naar aanleiding van de overlegde gegevens aanleiding ziet nader onderzoek te doen. Of, hetgeen zeer wel voorstelbaar is, dat de advocaat van de verdachte tijdens de zitting aandringt op nader onderzoek in het geval hij meent dat dit noodzakelijk is omdat het zijn cliënt kan ontlasten. Indien de advocaat dit aannemelijk kan maken zal de rechter zijn verzoek zeker toewijzen. Naast de al opgevraagde gegevens in het opsporingsonderzoek zullen dan ook andere bewaarde gegevens noodzakelijk kunnen zijn om met terugwerkende kracht verbanden bloot te leggen.

Als men zich voorts realiseert dat ook de rechter in hoger beroep nader onderzoek kan gelasten, zal het duidelijk zijn dat de bewaartermijn van achttien maanden die nu wordt voorgesteld, niets te lang zal zijn.

Statistische informatie

De richtlijn dataretentie legt aan de lidstaten de verplichting op ervoor te zorgen dat jaarlijks aan de Commissie statistische informatie wordt verstrekt over de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van diensten. Die informatie heeft betrekking op de gevallen waarin gegevens aan de bevoegde autoriteiten zijn verstrekt, de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard, de datum waarop door bevoegde autoriteiten om overdracht is verzocht en de gevallen waarin verzoeken niet konden worden ingewilligd.

In de memorie van toelichting is op bladzijde 14 een passage opgenomen waaruit blijkt dat het de bedoeling is dat van de verstrekking van gegevens, die niet via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) plaats vindt, door het openbaar ministerie zal kunnen worden geregistreerd. Het College is het eens met de constatering dat een dergelijke registratie nodig is om te kunnen voldoen aan de eis van de richtlijn. Maar het College stelt tevens vast dat het openbaar ministerie, om de volgende redenen, niet in staat zal zijn de gewenste registratie van de verkeersgegevens op zich te nemen. Ten eerste is het openbaar ministerie bij een deel van de opgevraagde gegevens niet betrokken. De politie kan zelfstandig de providers verzoeken NAW-gegevens te verstrekken. Ook van de verzoeken, gedaan door de veiligheidsdiensten is het openbaar ministerie niet op de hoogte. Hierdoor blijven belangrijke informatiestromen buiten beeld bij het openbaar ministerie. Ten tweede wijst het College wat betreft de gegevens die door de officier van justitie worden gevorderd op de volgende obstakels. De vordering tot het verstrekken van gegevens kan worden geregistreerd in COMPAS, het huidige bedrijfsprocessensysteem van het openbaar ministerie. In dit systeem kan echter niet worden geregistreerd of het verzoek al dan niet kon worden ingewilligd, dan wel wanneer antwoord op de vordering is gegeven. Ook de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop het openbaar ministerie de vordering heeft gedaan kan niet worden geregistreerd.

Bij de huidige inrichting van het wetsvoorstel, waarbij de gegevens decentraal worden opgeslagen, adviseert het College dat de gevraagde registratie door de providers dient te worden verzorgd. Zij beschikken al over alle gevraagde gegevens in verband met de facturering van de kosten die worden gemaakt ten behoeve van de verstrekking van gegevens. Het ligt dan voor de hand om ook de registratie van de door de richtlijn vereiste gegevens bij de providers te beleggen.

Bij een centrale geautomatiseerde opslag (zie volgende paragraaf) levert de gewenste registratie vrijwel geen problemen op en kan deze makkelijk worden gerealiseerd.

Centrale of decentrale opslag van gegevens

Met betrekking tot het vraagstuk van de centrale of decentrale opslag van gegevens merkt het College het volgende op. In de memorie van toelichting bij het wetsvoorstel wordt uitgelegd dat vooralsnog wordt voorgesteld om voor de implementatie van de richtlijn dataretentie van de bestaande situatie uit te gaan, dat wil zeggen decentrale opslag en bewaring van gegevens. Het College is echter een groot voorstander van een centrale opslag van gegevens, gelijk aan het systeem van de CIOT. Een centrale opslag van gegevens, onder beheer van de providers, die het mogelijk maakt om verkeersgegevens rechtstreeks elektronisch te bevragen. Ook het onderzoek van Verdonck, Klooster & Associates BV wijst uit dat centrale opslag van gegevens hoog scoort op het gebied van de kwalitatieve criteria zoals de beschikbaarheid van gegevens en de snelheid waarmee het systeem kan worden bevroegd. De kosten, verbonden aan de uitvoering van de richtlijn, zouden in het geval van centrale opslag door een derde partij lager kunnen zijn dan de kosten die nu door de providers moeten worden gemaakt omdat de gegevens decentraal worden opgeslagen.

Het College wijst er voorts op dat de uitvoering van de verplichte registratie van gegevens, zoals door de richtlijn vereist, eigenlijk alleen kan worden uitgevoerd bij een centrale opslag van gegevens.

Het College kan begrip opbrengen voor het feit dat op dit moment, teneinde de in de richtlijn gestelde implementatietermijn te halen, wordt gekozen voor een decentrale opslag van de gegevens. Maar het College dringt er tevens op aan dat tegelijkertijd de benodigde stappen worden gezet om te komen tot een centrale opslag van gegevens, naar het voorbeeld van de huidige CIOT-constructie. Alleen bij een centrale opslag en bewaring van gegevens is een snelle respons op een aanvraag gegarandeerd en kan ook ten volle aan de registratie-eisen worden voldaan.

De termijn voor verstrekking

Artikel 8 van de richtlijn dataretentie verplicht de lidstaten er voor te zorgen dat de gegevens op zodanige wijze worden bewaard dat de bewaarde informatie en alle daarmee verband houdende relevante informatie onverwijld aan de bevoegde autoriteiten kunnen worden meegedeeld wanneer daarom wordt verzocht.

In de memorie van toelichting wordt uitgelegd dat de Telecommunicatiewet thans niet voorziet in een termijn waarbinnen de gegevens door de aanbieders aan de bevoegde autoriteiten moeten worden verstrekt. Evenmin worden er regels gesteld voor de beschikbaarstelling van gegevens in geval van spoed. Er bestaan inmiddels wel afspraken tussen openbaar ministerie en politie enerzijds en de providers anderzijds ter zake van het verkrijgen van gegevens en het opnemen van telecommunicatie.

Het bestaan van deze afspraken neemt echter niet weg dat het College van oordeel is dat de wijze waarop de gegevens beschikbaar worden gehouden en de termijnen waarbinnen die gegevens beschikbaar moeten worden gesteld in een algemene maatregel van bestuur zullen worden opgenomen. Daarbij zou als vuistregel kunnen worden aangehouden dat in normale gevallen de gevraagde gegevens binnen 48 uur beschikbaar kunnen worden gesteld. Echter, in die gevallen waarin de bevoegde autoriteit van oordeel is dat het een zeer spoedeisend geval betreft, dienen de gegevens onverwijld ter beschikking te worden gesteld. En "onverwijld" heeft dan maar één betekenis, namelijk onmiddellijk. Het College dringt er op aan dat deze algemene maatregel van bestuur in overleg met het openbaar ministerie zal worden opgesteld.

Ook voor dit onderwerp geldt overigens dat bij centrale geautomatiseerde opslag en bewaring de onverwijfde beantwoording geen enkel probleem meer op zal leveren.

Hoogachtend

Het College van procureurs-generaal

H.N. Brouwer