



**RAAD VAN
DE EUROPESE UNIE**

**Brussel, 23 november 2004 (26.11)
(OR. en)**

15098/04

**Interinstitutioneel dossier:
2004/0813 (CNS)**

LIMITE

**COPEN 142
TELECOM 172**

NOTA

van:	het voorzitterschap
aan:	het Comité van permanente vertegenwoordigers/de Raad
nr. vorig doc.:	14713/04 COPEN 136 TELECOM 165
Betreft:	Ontwerp-kaderbesluit over de bewaring van gegevens die zijn verwerkt en opgeslagen in verband met het aanbieden van openbare elektronische-communicatiediensten of gegevens in openbare communicatienetwerken met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme

I INLEIDING

Frankrijk, Ierland, Zweden en het Verenigd Koninkrijk hebben op 28 april 2004 een voorstel ingediend voor een kaderbesluit over de bewaring van gegevens die zijn verwerkt en opgeslagen in verband met het aanbieden van openbare elektronische-communicatiediensten of gegevens in openbare communicatienetwerken met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme¹.

¹ 8958/04 CRIMORG 36 TELECOM 82 + EXT 1. Een toelichtende nota bij het voorstel volgt.

Het Europees Parlement is verzocht vóór eind februari 2005 advies uit te brengen over dit voorstel.

Het voorstel is op 4 juni, 27 en 28 september en 19 en 20 oktober 2004 in de Groep samenwerking in strafzaken en op 19 en 20 oktober en 11 en 12 november 2004 in het Comité van artikel 36 besproken. De recentste herziene versie van het voorstel staat in document 14190/1/04 REV 1 COPEN 132 TELECOM 160.

Het voorzitterschap verzoekt het Comité van permanente vertegenwoordigers/de Raad zich te buigen over het in de punten II, III en IV omschreven principiële vraagstuk aangaande de werkingssfeer van het instrument wat betreft de uit hoofde van het kaderbesluit te bewaren gegevens.

Opgemerkt zij dat diverse delegaties bij het voorstel algemene studievoorbehouden en algemene voorbehouden voor parlementaire behandeling hebben gemaakt en dat de Commissie haar standpunt aangaande de rechtsgrondslag van het voorstel in beraad houdt.

II ACHTERGROND

Inleiding

De justitiële en wetshandhavingsautoriteiten hebben zich de jongste jaren in toenemende mate bezorgd getoond over het gebruik voor criminele doeleinden van de technologische innovaties als gevolg van de gestage ontwikkeling van de elektronische communicatiediensten, alsook over de daaruit resulterende problemen op het gebied van de opsporing van en het onderzoek naar strafbare feiten. Deze bezorgdheid betreft niet alleen gesprekken met vaste telefoontoestellen, GSM's, Short Message Services (SMS), Electronic Media Services (EMS) en Multi Media Messaging Services (MMS), maar ook in toenemende mate internetprotocollen met inbegrip van e-mail, “voice over internet”, World Wide Web, “file transfer”-protocollen, “network transfer”-protocollen, “voice over broadband”, etc.

Het voorstel voor een kaderbesluit over de bewaring van gegevens ligt in het verlengde van met name de Verklaring van de Europese Raad van 25 maart 2004 betreffende de bestrijding van terrorisme ¹, die mede is afgelegd tegen de achtergrond van de conclusies van de Raad van 20 september 2001 ² en van 19 december 2002 ³ betreffende elektronische communicatiesystemen. In deze teksten zijn de bovengenoemde aandachtspunten, met name die in verband met het gebruik van telecommunicatie met het oogmerk terroristische daden te plegen, prominent aanwezig. In de verklaring van 25 maart 2004 is gesteld dat vóór juni 2005 een instrument over de bewaring van gegevens moet worden vastgesteld.

Na de eerste bijeenkomst van de groep op 4 juni 2004 heeft het toenmalige Ierse voorzitterschap de vragenlijst in document 10767/04 COPEN 77 TELECOM 125 verspreid om over meer gegevens te beschikken omtrent de juridische situatie in de verschillende lidstaten en de operationele behoefte aan bewaring van gegevens. De antwoorden op de vragenlijst staan in document 12076/04 COPEN 100 TELECOM 136.

De Commissie heeft twee workshops over de bewaring van gegevens gehouden, de eerste op 14 juni en de tweede op 21 september 2004. Deze workshops stonden niet alleen open voor deskundigen van de lidstaten, maar ook voor vertegenwoordigers van de industrie en andere betrokken partijen.

Uit de beschikbare informatie en de besprekingen die tot dusver hebben plaatsgevonden, blijkt dat de bewaring van gegevens een bijzonder ingewikkeld vraagstuk is om zowel politieke en juridische als praktische redenen:

¹ 7906/04 JAI 100 ECOFIN 107 TRANS 145 RELEX 123 ECO 73 PESC 208 COTER 20 COSDP 142.

² 12156/01 JAI 99.

³ 15763/02 CRIMORG 111.

- a. De juridische situatie is ingewikkeld, op het niveau van zowel de EU en de EG als nationaal. Maatregelen inzake gegevensbescherming moeten stroken met artikel 8 van het Europees Verdrag voor de rechten van de mens.¹ Al is inmenging in de uit hoofde van artikel 8, lid 1, beschermde rechten toegestaan op grond van artikel 8, lid 2, toch moet worden gekeken naar de voorwaarden waaronder dit geschiedt, de juridische waarborgen en de evenredigheid van de maatregel.
- b. Hoewel niet rechtstreeks van toepassing in de derde pijler, moet tevens rekening worden gehouden met het ter zake geldende EG-recht, waaronder met name Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie.
- c. Het recht en de praktijk in verband met het bewaren van verkeersgegevens voor wets-handhavingsdoeleinden zijn zeer verschillend van lidstaat tot lidstaat. Gegevensbescherming en privacy staan centraal in de besprekingen.
- d. De technische implicaties zijn complex. De verschillende soorten telecommunicatie worden in verschillende technische systemen gebruikt. Zowel de door de dienstenleveranciers gebruikte technologie - hardware én software - als de diensten die aan de gebruikers van telecommunicatiediensten worden aangeboden, zijn voortdurend aan snelle veranderingen onderhevig. De belangen van de dienstverleners, waaronder het kostenvraagstuk, moeten in aanmerking worden genomen.
- e. De belangenafweging (wetshandhaving versus andere belangen zoals de belangen van de industrie en gegevensbescherming) die binnen het bestek van de juridische en technische mogelijkheden moet worden gemaakt, ligt politiek gevoelig.

¹ "Artikel 8 - Eerbiediging van het privé-leven en het familie- en gezinsleven

- 1. Een ieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
- 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voorzover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."

Werkingssfeer met betrekking tot de te bewaren gegevens

Het voorstel houdt in beginsel in, dat de aanbieders van openbare elektronische-communicatiediensten of -netwerken welbepaalde gegevens moeten bewaren waarmee de bron, de routing, de bestemming, het tijdstip en de duur van een communicatie kunnen worden vastgesteld en de locatie van de gebruikte telecommunicatieapparatuur kan worden bepaald. In de oorspronkelijke versie van het voorstel leek het alleen te gaan om gegevens die reeds waren verwerkt en opgeslagen met het oog op facturering, commerciële of andere legitieme doeleinden. Het oorspronkelijke voorstel leek met name in te houden dat de gegevens die de dienstverleners besloten hebben niet te bewaren voor facturerings- of marketingdoeleinden in de zin van Richtlijn 2002/58/EG, buiten de werkingssfeer van het kaderbesluit zouden vallen.

Deze aanpak zou erop neerkomen dat de mogelijkheid om voor wetshandavingsdoeleinden toegang te krijgen tot gegevens bepaald wordt door de technische en commerciële inrichting van de diverse betrokken dienstverleners. Of dit een goede zaak is, is maar al te zeer de vraag, omdat sommige dienstverleners systemen, zoals forfaitaire systemen, kunnen toepassen, die er mogelijkwijs op neerkomen dat de relevante gegevens, die worden verwerkt om de bewuste telecommunicatiedienst te kunnen verrichten, onmiddellijk na het beëindigen van de communicatie worden gewist. Een aantal delegaties is van oordeel dat het bewaren van de desbetreffende gegevens niet van dergelijke omstandigheden mag afhangen. Vele van deze delegaties hebben er evenwel op gewezen dat dienstverleners niet verplicht mogen worden gegevens te bewaren die zij thans zelfs niet verwerken/genereren. Alleen gegevens die voor telecommunicatiedoeleinden worden verwerkt/gegenereerd en aldus ten minste tijdelijk in het systeem van de dienstverlener aanwezig zijn, mogen in de werkingssfeer worden opgenomen. Ook is geopperd dat de verplichting om gegevens te bewaren, gedifferentieerd moet worden naargelang van het type telecommunicatie, met name ten aanzien van de bewaarperiodes.

III OPTIES DIE IN HET COMITE VAN ARTIKEL 36 ZIJN BESPROKEN

In de vergadering van 22 november 2004 heeft het Comité van artikel 36 besproken welke van de twee volgende opties de basis zou moeten vormen voor de verdere onderhandelingen. Hoe de gekozen optie precies in praktijk wordt gebracht wat betreft de verschillende soorten telecommunicatie (voice phone, internet, etc.), de lijst van de te bewaren gegevens (artikel 2, lid 2), de periodes voor de bewaring (artikel 4), alsook een aantal andere nog niet opgeloste vraagstukken, is een vraag die nadien in het licht van de gegeven instructies op technisch niveau kan worden besproken.

Optie 1

De aan dienstverleners opgelegde verplichting tot bewaring van gegevens moet worden beperkt tot de gegevens die tijdens het verstrekken van de desbetreffende telecommunicatiedienst door de dienstverlener worden verwerkt/gegenereerd en vervolgens voor facturering of voor commerciële of andere legitieme doeleinden worden opgeslagen.

Voordelen: Dit is een eenvoudige aanpak, die de kans vergroot dat de deadline van juni 2005 voor de aanneming van de maatregel wordt gehaald. De kosten zijn relatief beperkt. Deze optie zal wellicht aanleiding geven tot minder evenredigheidsbezwaren dan optie 2.

Nadelen: Het zwakke punt van deze aanpak is de afhankelijkheid van het commerciële gedrag van de dienstverleners en de technische ontwikkelingen die dat gedrag beïnvloeden. Bovendien zou het tot concurrentievervalsing kunnen leiden. Het zou ook kunnen impliceren dat misdadigers gebruik maken van dienstverleners die minder gegevens bewaren dan andere.

Optie 2

De aan dienstverleners opgelegde verplichting tot het bewaren van gegevens moet gelden voor alle relevante gegevens zoals omschreven in een gemeenschappelijke lijst in het rechtsinstrument¹, mits de gegevens door de dienstverlener worden verwerkt/gegenereerd tijdens het verrichten van de desbetreffende communicatiedienst.

Voordelen: Deze aanpak kan meer zekerheid bieden wat de bewaring van de relevante gegevens betreft en is minder onderhevig aan het commerciële gedrag van de dienstverlener en de technische ontwikkelingen. De dienstverlener zou verplicht zijn de desbetreffende gegevens te bewaren voor zover de gegevens door hem worden verwerkt/gegenereerd, zelfs als de gegevens voor hem niet van belang zijn. Deze aanpak zou tot een relatief hoge graad van harmonisatie van de wetgeving der lidstaten leiden.

Nadelen: Deze aanpak kan de onderhandelingen over details bemoeilijken. Er kunnen grotere bezwaren tegen worden aangevoerd die verband houden met evenredigheid, kosten voor het bewaren van de gegevens en gegevensbescherming, enz.

In het Comité van artikel 36 was een ruime meerderheid van de delegaties voor optie 2, zoals omschreven in de vergadering. Een aantal van die delegaties onderstreepte dat het belangrijk is een lijst van te bewaren gegevens op te stellen die algemene toepassing zou vinden. Ook het kosten-vraagstuk kwam aan de orde. De Commissie vond het het overwegen waard een minder complexe procedure in te stellen om in voorkomend geval sommige bepalingen op details te wijzigen, gezien de technologische en commerciële ontwikkelingen. Een minderheid van de delegaties gaf de voorkeur aan optie 1. In het licht van opmerkingen van andere delegaties toonden de meeste van die delegaties zich echter bereid om optie 2 te bespreken.

¹ Artikel 2, lid 2, van het ontwerp bevat een opsomming van de te bewaren gegevens (gegevens waarmee de bron, de routing, de bestemming, het tijdstip en de duur van een communicatie kunnen worden vastgesteld en de locatie van de gebruikte telecommunicatieapparatuur kan worden bepaald). Deze bepaling moet nader worden bestudeerd.

IV CONCLUSIE

Het voorzitterschap verzoekt de Raad ermee in te stemmen dat het voorstel in dit stadium verder moet worden besproken op basis van optie 2, zonder uit te sluiten dat het onderwerp in een later stadium opnieuw aan de orde komt, naargelang van de vragen die tijdens de verdere technische behandeling van de tekst zouden kunnen opduiken.
