RAAD VAN DE EUROPESE UNIE

Brussel, 20 december 2004 (07.01)
(OR. en)

8958/04
ADD 1

CRIMORG 36
TELECOM 82

ADDENDUM BIJ HET INGEKOMEN DOCUMENT

van:	de Franse republiek, Ierland, het Koninkrijk Zweden en het Verenigd Koninkrijk
d.d.:	28 april 2004
aan:	Javier Solana, secretaris-generaal/hoge vertegenwoordiger
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

Hierbij gaat voor de delegaties de toelichting bij bovengenoemd initiatief.

TOELICHTING
KADERBESLUIT OVER DE
BEWARING VAN COMMUNICATIEGEGEVENS
(doc. 8958/04)

1. INLEIDING

Bewaring van gegevens

Onder "bewaring van gegevens" wordt de opslag verstaan van communicatiegegevens die door aanbieders van telecommunicatiediensten worden geproduceerd bij het verstrekken van hun algemene diensten. De duur van de bewaring van de gegevens door individuele aanbieders van telecommunicatiediensten varieert naar gelang van een aantal factoren, waaronder de behoeften van het bedrijfsleven, het platformvermogen, de platformcapaciteit en de nationale wetgeving. Momenteel zijn er in Europa, zowel tussen de lidstaten onderling als binnen de lidstaten, grote verschillen inzake duur van de bewaring van communicatiegegevens door aanbieders van telecommunicatiediensten.

Achtergrond

De Europese Unie, die uit stedelijke samenlevingen bestaat met kwetsbare infrastructuren en open grenzen, dreigt steeds meer het slachtoffer te worden van grensoverschrijdende criminele activiteiten. De noodzaak van een Europawijd beleid inzake gegevensbewaring werd voor het eerst erkend in een reactie op deze toename van de omvang van de internationale criminaliteit.

Tegelijkertijd komt dit kaderbesluit echter ook op een ogenblik dat de dreiging die van het terrorisme uitgaat, scherp in beeld komt. De bomaanslagen te Madrid op 11 maart 2004 waren voor Europa een levendige illustratie van de ernstige dreiging die nu voor de lidstaten uitgaat van radicale terroristische groeperingen. Deze toenemende dreiging van terroristische aanslagen is niet de voornaamste basis voor de noodzaak van een Europawijd beleid inzake gegevensbewaring, maar creëert, voedt en versterkt wel het gevoel dat er dringend actie moet worden ondernomen. Dit kaderbesluit is dan ook zowel tegen criminele activiteiten in het algemeen als tegen terroristische daden gericht.

Het is duidelijk dat hoog georganiseerde internationale criminele en terroristische organisaties, die op de hoogte zijn van de onderlinge verschillen tussen de wettelijke voorschriften van de lidstaten op het gebied van gegevensbewaring, onvermijdelijk zullen worden aangetrokken door lidstaten waar de verplichte duur van bewaring van de gegevens door aanbieders van telecommunicatiediensten het kortst is. De reden daarvoor is uiteraard om te profiteren van de aldus verschafte anonimiteit en op die manier de inspanningen te dwarsbomen van onderzoekers die hun "communicatiesporen" proberen te volgen om hen op de plaats van het strafbare feit te situeren of om alle medeplichtigen en samenzweerders te identificeren. De onderlinge aanpassing van de voorschriften inzake bewaring verkleint het risico van het ontstaan van dergelijke "gegevensvrijhavens" binnen de Europese Unie en, misschien belangrijker nog, zorgt ervoor dat bewijzen in de vorm van communicatiegegevens beschikbaar zijn om de justitiële samenwerking tussen de wetshandhavingsinstanties te vergemakkelijken.

Juist nu de dreiging van de kant van internationale criminelen en terroristen is toegenomen, hebben zich tegelijkertijd ook aanzienlijke technologische wijzigingen voorgedaan in de telecommunicatiesector, waar scherpe concurrentie heerst. Door deze ontwikkelingen worden de aanbieders van diensten onder druk gezet om de duur van de bewaring van communicatiegegevens te beperken. Een van de nieuwe technologieën die reeds invloed hebben op de bewaarperiode van gegevens is de technologie met betaling op gebruiksbasis. Dit is een van belangrijkste drijfveren om de duur van de bewaring van communicatiegegevens door de sector te verminderen; bovendien kan deze betalingsoptie in ieder geval de oorspronkelijk beschikbare hoeveelheid gegevens beperken.

Deze technologische ontwikkelingen komen bovenop de steeds toenemende commerciële eisen die de bedrijven ertoe nopen de waarde en de doeltreffendheid van hun systemen voortdurend te evalueren en opnieuw te evalueren. Deze commerciële druk om de kosten laag te houden betekent ook dat communicatiegegevens die voorheen voor bedrijfsdoeleinden werden bijgehouden, nu worden vernietigd omdat de commerciële waarde ervan gedaald is. Het is duidelijk dat deze druk weliswaar bestaat en toeneemt, maar in veel bedrijven nog geen "kritische massa" heeft bereikt, en dat de bewaarperiode wel verkort, maar nog niet drastisch verkort is. Met dit kaderbesluit wordt vooruitgelopen op deze eventualiteit. Uit voorafgaand onderzoek blijkt ook dat aanbieders van telecommunicatiediensten de bewaarperiode voor bepaalde soorten gegevens wellicht zullen moeten verlengen, maar dat het onwaarschijnlijk is dat alle bedrijven de bewaringsduur voor alle soorten gegevens zullen moeten verlengen om aan dit kaderbesluit te voldoen.

Om de lidstaten in staat te stellen een ruimte van vrijheid, veiligheid en rechtvaardigheid te waarborgen en te slagen in hun strijd tegen de criminaliteit, met inbegrip van terrorisme, is het dan ook van essentieel belang dat wetgeving wordt ingevoerd die alle lidstaten verplicht bindende bepalingen inzake de bewaring van gegevens op te stellen. Gezien het internationale karakter van de bedrijfstak van aanbieders van telecommunicatiediensten, strekt dit kaderbesluit dan ook tot de onderlinge aanpassing van de voorschriften van de lidstaten om te waarborgen dat dit essentiële onderzoeksinstrument beschikbaar is ingeval van een strafbaar feit of een terroristische daad.

Doel van dit kaderbesluit

Aanbieders van telecommunicatiediensten produceren bij de dagelijkse verrichting van hun diensten communicatiegegevens. Deze gegevens worden momenteel opgeslagen om een aantal redenen, waaronder opsporing van fraude, facturatie en naleving van financiële regelgeving. Dit kaderbesluit bevat maatregelen die de aanbieders van telecommunicatiediensten verplichten de duur van de bewaring voor bepaalde van deze soorten gegevens te handhaven of te verlengen.

De jongste jaren is de steun voor de invoering van bindende voorschriften inzake bewaring van communicatiegegevens toegenomen en in een stroomversnelling geraakt. Het pleit is nu beslecht en het belang van communicatiegegevens als onderzoeksinstrument wordt nagenoeg algemeen erkend en in een aantal fora geaccepteerd. Hieronder volgen enkele van de wellicht belangrijkste en recentste.

Op 20 september 2001 heeft de Raad zijn goedkeuring gehecht aan conclusies (document SN 3926/6/01) waarin het belang van communicatiegegevens bij de bestrijding van criminaliteit en terrorisme wordt erkend. Voorts heeft hij de Europese Commissie verzocht voorstellen in te dienen om ervoor te zorgen dat de wetshandhavingsinstanties de mogelijkheid hebben om strafbare feiten te onderzoeken die het gebruik van elektronische communicatiesystemen omvatten.

Het belang van communicatiegegevens wordt voorts erkend in artikel 15 van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie, dat de lidstaten toestaat wettelijke maatregelen te treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9, van de richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG.

Tijdens zijn zitting van 19 december 2002 heeft de Raad conclusies over informatietechnologie en onderzoek en vervolging ter zake van georganiseerde criminaliteit aangenomen (document 15691/02). In deze conclusies werd gesteld dat het behoud en de ontwikkeling van de Unie als ruimte van vrijheid, veiligheid en rechtvaardigheid, als bepaald in artikel 2 van het Verdrag betreffende de Europese Unie, en het scheppen van een hoog niveau van veiligheid in deze ruimte, zijnde de algemene doelstelling van artikel 29 van het Verdrag, veronderstelt dat strafrechtelijk onderzoek en vervolging in voldoende mate, grondig en doeltreffend kunnen worden uitgevoerd, onder eerbiediging van de mensenrechten en de fundamentele vrijheden van artikel 6 van het Verdrag betreffende de Europese Unie.

In deze conclusies werd ook met bezorgdheid geconstateerd dat de technologische vernieuwingen die de permanente ontwikkeling van het internet en andere elektronische-communicatiediensten samen met het toegenomen elektronische bankverkeer met zich meebrengen, de samenleving aanzienlijke voordelen opleveren, maar tegelijk misdadigers, en in het bijzonder criminele organisaties, steeds meer mogelijkheden bieden.

Voorts werd er in deze conclusies bij alle betrokken partijen (regeringen, parlementen, wets-handhavingsinstanties en justitiële autoriteiten, bedrijfsleven, gegevensbeschermings-autoriteiten en andere betrokken partijen) op aangedrongen om, als een zaak van prioritair belang, op nationaal en EU-niveau een open en constructieve dialoog aan te gaan waarin wordt gezocht naar oplossingen voor het bewaren van verkeersgegevens die tegemoet komen aan de behoefte aan doeltreffende instrumenten voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten en die tevens in overeenstemming zijn met de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, in het bijzonder met het recht op persoonlijke levenssfeer, gegevensbescherming en vertrouwelijkheid van communicatie.

Op 25 maart 2004 heeft de Europese Raad een verklaring betreffende de bestrijding van terrorisme gepubliceerd, waarin werd gewezen op het belang van het opstellen van voorschriften voor het bewaren van verkeersgegevens door telecommunicatieaanbieders. Voorts werd gesteld dat voorrang moet worden gegeven aan het opstellen van dit voorstel, zodat dit voor juni 2005 kan worden aangenomen.

Rechtsgrondslag van het kaderbesluit

De rechtsgrondslag van het kaderbesluit is het Verdrag betreffende de Europese Unie, met name artikel 31, lid 1, onder c), en artikel 34, lid 2, onder b).

Vastlegging van gegevens is geen alternatief voor bewaring van gegevens

In het standpunt van de Europese functionarissen voor de gegevensbescherming, dat gepubliceerd is in de vorm van Advies 5/2002, wordt gepleit voor vastlegging in plaats van bewaring van gegevens. Vastlegging van gegevens is de opslag van gegevens betreffende welbepaalde personen, eerder dan de allesomvattende opslag van gegevens uit hoofde van een regeling inzake bewaring van gegevens. De door de functionarissen voor gegevensbescherming voorgestelde vastlegging van gegevens wordt door de veiligheids-, inlichtingen- en wetshandhavingsdiensten als zeer nuttig erkend voor het onderzoek naar de activiteiten van iemand die reeds onder verdenking staat. Het zal echter nooit bijdragen tot het onderzoek naar een persoon die niet reeds verdacht wordt van betrokkenheid bij een criminele of terroristische organisatie.

De vastlegging van gegevens volstaat bijgevolg niet om te voldoen aan de behoeften van de veiligheids-, inlichtingen- en wetshandhavingsinstanties bij de bestrijding van moderne criminelen, waaronder terroristen.

Voorts voorkomt het bestaan van een regeling voor de bewaring van gegevens, dat buitensporig gebruik wordt gemaakt van de vastlegging van gegevens. Een wezenlijk aspect van de bewaring van gegevens dat vaak verkeerd begrepen wordt, is het volgende: in de regeling voor de bewaring van gegevens wordt ervan uitgegaan dat bewaarde gegevens in principe niet toegankelijk zijn voor om het even wie. De wetshandhavingsinstanties mogen slechts voor een zeer beperkt deel van deze gegevens, en dan nog per geval, beslissen deze informatie in te zien. Zonder deze regeling en rekening houdend met de dreigingen van nieuwe vormen van criminaliteit, waaronder terrorisme, zou er steeds meer behoefte zijn aan uitbreiding van de vastlegging van gegevens, waarbij alle van of naar een specifieke persoon verstuurde informatie niet alleen wordt bewaard, maar ook kan worden geraadpleegd door de autoriteit die opdracht tot de vastlegging heeft gegeven.

2. ARTIKEL 1 - WERKINGSSFEER EN DOELSTELLING

Dit kaderbesluit heeft tot doel te garanderen dat gegevens die tijdens het tot stand brengen of ontvangen van communicaties worden geproduceerd, voor een vastgestelde duur worden bewaard door de aanbieders van telecommunicatiediensten teneinde zo later onderzoek van de communicatiegegevens mogelijk te maken en de justitiële samenwerking te vergemakkelijken, indien daartoe een legitieme behoefte bestaat met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten, daaronder begrepen terrorisme.

Dit artikel bepaalt wat wel en niet onder de werkingssfeer van dit kaderbesluit valt. Dit kaderbesluit handelt niet over het onderscheppen van de inhoud van communicaties. Met andere woorden, dit kaderbesluit heeft geen betrekking op wat eigenlijk wordt gezegd of geschreven in een communicatie.

De doeleinden waarvoor communicatiegegevens uit hoofde van het kaderbesluit kunnen worden bewaard, staan in artikel 15 van Richtlijn 2002/58/EG. Zoals hierboven reeds is aangehaald, behoren het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten tot deze doeleinden.

De doelstelling van "het voorkomen van strafbare feiten" is misschien de enige die niet voor zichzelf spreekt en tot verwarring kan leiden. Het voorkomen van strafbare feiten in het kaderbesluit heeft alleen betrekking op situaties waarin redelijkerwijs kan worden vermoed dat er een strafbaar feit wordt gepland. Met andere woorden, de verdachten moeten een redelijk vermoeden hebben doen rijzen dat een strafbaar feit zal worden begaan; op grond daarvan stellen de wetshandhavingsinstanties een onderzoek in naar de verdachten om hun plannen te verijdelen. Het begrip "voorkomen van strafbare feiten" in het kaderbesluit is niet beperkt in de zin van de soorten criminaliteit die onder de werkingssfeer van het kaderbesluit vallen.

Binnen het kaderbesluit wordt echter ook erkend dat er binnen de Europese Unie verschillende juridische standpunten zijn met betrekking tot "het voorkomen van strafbare feiten" als doel voor de bewaring van gegevens. In het kaderbesluit wordt gepoogd deze verschillen te overbruggen door te erkennen dat het voor sommige lidstaten misschien niet wenselijk is het beginsel van de bewaring van gegevens met het oog op "het voorkomen van strafbare feiten" aan te nemen, onder meer omdat "het voorkomen van strafbare feiten" niet tot de bevoegdheid behoort van de autoriteiten die zich bezighouden met speciale onderzoeksmaatregelen die het verwerven van communicatiegegevens omvatten. Daarom is in het kaderbesluit in een afwijking voorzien waarbij de lidstaten ervoor kunnen kiezen "het voorkomen van strafbare feiten" als doelstelling van de bewaring van gegevens uit te sluiten van hun nationale recht.

3. ARTIKEL 2 - DEFINITIES VAN GEGEVENS

Tot de gegevens die momenteel door de communicatiesector worden opgeslagen, behoort een breed scala van gegevens die zij in de eerste plaats nodig hebben voor het beheer van de exploitatie van hun netwerken en voor facturatiedoeleinden. Deze informatie is opgenomen in artikel 2 van het kaderbesluit en identificeert "wie wanneer, waar en hoe welke oproep heeft gedaan" op ieder netwerk of bij iedere dienst. Elk bedrijf kan voor verschillende gegevens pasklare bewaringsbehoeften hebben en voor het onderzoek naar criminele en terroristische activiteiten moeten de volgende gegevens worden bewaard voor de in artikel 1 genoemde doeleinden (zie kaderbesluit): de telefoonnummers, internetadressen en facturatieadressen van de klanten en de telefoonnummers/communicaties die vanaf een bepaald telefoontoestel/een bepaalde computer zijn opgebeld/tot stand gebracht.

Daarnaast vallen onder het kaderbesluit ook de gegevens betreffende het tijdstip van een oproep/communicatie, de duur van een oproep/communicatie en de plaats van het oproepende en het ontvangende telefoontoestel.

4. ARTIKEL 3 - BEWARING VAN GEGEVENS

In dit artikel staat dat alle lidstaten deze maatregelen moeten treffen ter vergemakkelijking van de internationale justitiële samenwerking inzake strafbare feiten, waaronder terrorisme, wanneer er sprake is van criminele gedragingen of bewijzen van criminaliteit met een grensoverschrijdend karakter.

5. ARTIKEL 4 - DUUR VAN DE BEWARING VAN GEGEVENS

Dit artikel bepaalt dat alle lidstaten de nodige wetgeving moeten invoeren om ervoor te zorgen dat communicatiegegevens gedurende ten minste twaalf maanden en ten hoogste zesendertig maanden worden bewaard. Een gemeenschappelijke minimale bewaarperiode is noodzakelijk voor een betere justitiële samenwerking in strafzaken.

Dit artikel behelst ook een afwijking om de individuele lidstaten de mogelijkheid te bieden deze periodes in bepaalde omstandigheden te laten variëren voor specifieke technologieën, waartoe telefonie niet behoort, maar bijvoorbeeld wel text messaging en e-mail. Wanneer de lidstaten ervoor kiezen gebruik te maken van deze afwijking, kunnen zij de bewaarperiode met betrekking tot deze technologieën verlengen of verkorten.

6. ARTIKEL 5 - TOEGANG TOT GEGEVENS

Dit artikel heeft tot doel gebruik te maken van de instrumenten betreffende justitiële samenwerking waarbij de lidstaten reeds partij zijn en die van toepassing zijn op aangelegenheden die onder het kaderbesluit vallen, zoals de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, ondertekend op 29 mei 2000 (de Europese Raad heeft er in zijn verklaring van 26 maart 2004 bij de lidstaten op aangedrongen deze voor eind 2004 te bekrachtigen).

7. ARTIKEL 6 - GEGEVENSBESCHERMING

Dit artikel vormt een essentieel onderdeel van het kaderbesluit, dat er niet alleen op gericht is de doeltreffendheid van onze nationale systemen bij de bestrijding van criminaliteit te verbeteren, maar ook te garanderen dat deze verenigbaar is met de beginselen van privacy en gegevensbescherming.

Het artikel gaat uit van de beginselen van gegevensbescherming die in andere EU- en internationale instrumenten zijn opgenomen, met name in Richtlijn 95/46/EG. Het vestigt de aandacht op de noodzaak en de proportionaliteit van de toegang tot de gevraagde gegevens en op de noodzaak om met betrekking tot de toegang tot communicatiegegevens per geval beslissingen te nemen in overeenstemming met het nationale recht van de individuele lidstaat.

8. ARTIKEL 7 - GEGEVENSBEVEILIGING

Dit artikel betreft de integriteit en het vermogen om de voortdurende integriteit van de bewaarde communicatiegegevens te waarborgen. Het is van essentieel belang dat de communicatiegegevens tijdens de volledige bewaarperiode volgens dezelfde normen worden bewaard op het netwerk van de aanbieders van telecommunicatiediensten. Het artikel bepaalt voorts dat de procedure van toegang tot die gegevens duidelijk moet worden omschreven in het nationale recht van de individuele lidstaat.

9. ARTIKEL 8 - UITVOERING

Dit artikel maakt duidelijk dat het tijdens het uitvoeringsproces van essentieel belang zal zijn dat iedere lidstaat met de aanbieders van telecommunicatiediensten binnen zijn jurisdictie besprekingen voert over de bepalingen van het kaderbesluit.