

Bewaren telecommunicatieverkeer verplicht vanaf juli 2007

OP 21 FEBRUARI 2006 KEURDE DE EUROPESE RAAD EEN VOORSTEL VAN RICHTLIJN GOED DAT TELECOM- EN INTERNETBEDRIJVEN VERPLICHT OM VANAF JULI 2007 DE VERKEERSGEVENS TE BEWAREN VAN ALLE GESPREKKEN VIA TELEFOON OF GSM EN COMMUNICATIE VIA INTERNET. DEZE RICHTLIJN ZAL DE PRIVACY OP SIGNIFICANTE WIJZE BEPERKEN. MAAR OF HET OPSLAAN VAN HET TELECOMMUNICATIEVERKEER OOK ZAL HELPEN IN DE STRIJD TEGEN DE ZWARE CRIMINALITEIT, IS HOOGST ONZEKER.

Joris Deene

Als zoveelste post-9/11 maatregel wilde de Europese Commissie de opsporingsdiensten meer armslag geven in hun strijd tegen het terrorisme, zeker na de aanslagen in Londen. De richtlijn maakt het onderzoeken, opsporen en vervolgen van zware criminaliteit gemakkelijker door verkeers- en locatiegegevens beschikbaar te maken. Aanvankelijk had deze richtlijn ook betrekking op de proactieve recherche ter voorkoming van misdaden, maar dat aanvaardde het Europese parlement niet, omdat het begrip 'voorkomen' te vaag is en tot misbruik van het systeem kan leiden.

Welke gegevens moeten worden bewaard? Alle gegevens die nodig zijn om te achterhalen wie met wie, wanneer en van welke plek, hoe en hoelang gebeld heeft, voor wie een sms- of e-mailbericht bestemd is en hoe groot dit bericht was, hoelang u ingelogd was bij uw internet provider, welke webpagina's u heeft bezocht. Belangrijke beperking is dat gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, niet mogen worden bewaard.

Gegevens over de oproeping zonder resultaat (een communicatie waarbij een telefoonoproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord) moeten worden opgeslagen. Gegevens over niet tot stand gekomen verbindingen niet.

De richtlijn laat een keuzevrijheid aan de lidstaten voor de termijn waarbinnen verkeers- en locatiegegevens moeten worden bewaard. De minimale bewaartijd is zes maanden. Langer dan twee jaar kan bewaring van telecommunicatieverkeer niet verplicht worden.

De lidstaten moeten de extra kosten, die telecomaانبieders maken voor het bewaren, opslaan en doorzenden van gegevens, niet vergoeden. Nochtans kunnen de bewaarkosten hoog oplopen.

BELGIË

Nog voor de goedkeuring van de richtlijn zijn in België initiatieven in die zin genomen. Zo stelt artikel 126 van de wet op de elektronische communicatie van 13 juni 2005 dat de ministerraad bij kb de voorwaarden kan vastleggen waaronder operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers moeten registreren en bewaren. Tot op heden is een dergelijk kb er nog niet.

De Belgische regeling, zoals die uit de wet blijkt, is veel ruimer dan die van de Europese richtlijn. Zo kan aan operatoren gevraagd worden om gegevens op te slaan met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik maken van een elektronisch communicatienetwerk of -dienst. De bewaarperiode kan door de ministerraad vrij worden vastgelegd, maar mag wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden zijn.

VEILIGHEID

De lidstaten moeten er voor zorgen dat de aanbieders van elektronische communicatiediensten of van een publiek communicatienetwerk een aantal beginselen van gegevensbeveiliging respecteren. De toekomst zal uitwijzen of de databanken waarin de gegevens worden opgeslagen voldoende technisch beveiligd zullen zijn. In ieder geval moet elke lidstaat er voor zorgen dat één of meer overheidsinstanties verantwoordelijk worden gesteld voor het monitoren van de veiligheid van de bewaarde gegevens. Deze instanties moeten volledig onafhankelijk werken.

De lidstaten moeten er zorg voor dragen dat de bewaarde gegevens enkel in specifieke gevallen en in overeenstemming met de nationale wetgeving aan de bevoegde nationale autoriteiten worden meegedeeld. De niet toegestane toegang of overbrenging van gegevens moet beteugeld worden met administratieve of strafrechtelijke sancties die effectief, evenredig en afschrikkend zijn. Tot slot kunnen lidstaten met specifieke omstandigheden die een beperkte verlenging van de bewaringsplicht rechtvaardigen, noodzakelijke maatregelen treffen. De lidstaat dient dan wel de Commissie en de overige lidstaten onverwijld in kennis te stellen van de genomen maatregelen, met vermelding van de redenen voor dat besluit.

EFFECTIEF

Niemand zal betwisten dat de strijd tegen de zware criminaliteit het bewaren van gegevens over het telecommunicatieverkeer noodzakelijk maakt. De vraag is echter of deze richtlijn hiertoe een effectief instrument is.

Het zal dikwijls voorkomen dat de gebruiker niet met de bewaarde gegevens kan worden geïdentificeerd. Dit is bijvoorbeeld het geval als er gebeld wordt met gestolen gsm's of *prepaid* gsm's (waarmee tegenwoordig ook op het internet gesurft kan worden). Het is vaak moeilijk om het internetverkeer dat door de abonnee van een *internet provider* wordt veroorzaakt, te koppelen aan de persoon die daadwerkelijk van de internetverbinding gebruik gemaakt heeft. Denk bijvoorbeeld aan internetcafés of aan draadloze wifi-netwerken die al dan niet met de toestemming van de abonnee worden gebruikt om toegang tot het net te krijgen. Wie anoniem wil chatten of mailen, kan dit doen vanuit een website die buiten de EU staat. De *internet access provider* zal weliswaar registreren naar welke website gesurft wordt, maar niet met wie de abonnee in contact staat. Daarnaast bestaan nog tal van andere mogelijkheden, zoals het draaien van een eigen server of het werken via besloten netwerken, anonieme *proxies*, *freenet* en versleutelde tunnels.

De echte criminelen, die deze richtlijn viseert, zullen met het in de arm nemen van ervaren informatici de dans ontspringen. De doorsnee burger zal er een zware prijs voor betalen. Deze richtlijn zal de privacyomvang van de rechtsonderhorigen op significante wijze beperken. Het Europese parlement was zich terdege bewust van de potentiële gevaren van deze richtlijn en heeft een moedige poging gedaan om het ingrijpende karakter ervan te verzachten door veiligheidsvoorschriften in te lassen en niet-geautoriseerd gebruik van de gegevens strafbaar te stellen. De vraag is of deze bepalingen geen doekje voor het bloeden zijn. '*Quis custodiet ipsos custodes?* (Wie zal de bewakers zelf bewaken)' verwoordde Juvenalis het ooit. Deze vraag dient vandaag de dag meer dan ooit van haar retorisch karakter ontbloot te worden.

(De auteur is assistent aan de Universiteit Gent en advocaat)

Richtlijn 2005/0182 (COD) van het Europese Parlement en de Raad betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG - Deze richtlijn werd door het Europese Parlement op 14 december 2005 en door de Europese Raad op 21 februari 2006 goedgekeurd en zal spoedig in het EG-publicatieblad worden gepubliceerd.