EUROPESE COMMISSIE

Brussel, 13.7.2011
COM(2011) 429 definitief

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Een Europees systeem voor het traceren van terrorismefinanciering: beschikbare opties

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Een Europees systeem voor het traceren van terrorismefinanciering: beschikbare opties

1. INLEIDING

Toen de Raad instemde met de sluiting van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het programma voor het traceren van terrorismefinanciering (EU-VS TFTP-overeenkomst)[1], verzocht hij de Commissie tevens uiterlijk een jaar na de datum van inwerkingtreding van de overeenkomst (1 augustus 2010) "een juridisch en technisch kader voor het extraheren van gegevens op het EU-grondgebied" voor te leggen aan het Europees Parlement en de Raad[2]. Het Europees Parlement heeft er ook herhaaldelijk op aangedrongen op langere termijn een duurzame, juridisch verantwoorde Europese oplossing te bieden voor het extraheren van de gevraagde gegevens op Europees grondgebied.[3] In haar mededeling "De EU-interneveiligheidsstrategie in actie: vijf stappen voor een veiliger Europa" heeft de Commissie ook al verklaard dat zij in 2011 een beleid voor de EU zal ontwikkelen inzake het opvragen en analyseren van gegevens betreffende het financiële berichtenverkeer op haar eigen grondgebied[4]. Het Amerikaanse TFTP heeft zijn nut bewezen; een Europees systeem moet ertoe leiden dat pogingen om terroristen de toegang tot financiering en materiaal onmogelijk te maken en hun transacties te volgen, vrucht afwerpen. Voorts staat in artikel 11 van de EU-VS TFTP-overeenkomst dat de Europese Commissie tijdens de geldigheidsduur van de overeenkomst een studie zal uitvoeren naar de mogelijke invoering van een soortgelijk EU-systeem, dat een meer gerichte doorgifte van gegevens mogelijk zou maken. Deze mededeling is een eerste reactie van de Commissie op dit artikel en op het verzoek van de Raad. In de mededeling worden de verschillende stappen beschreven die de Commissie heeft ondernomen om een "juridisch en technisch kader" in het leven te roepen; tevens worden de verschillende opties gepresenteerd die worden overwogen om dit doel te verwezenlijken. In deze fase wordt nog geen voorkeur voor een bepaalde optie uitgesproken – wel worden de punten beschreven waarmee rekening moet worden gehouden bij de verschillende opties. Gezien het politieke belang van dit onderwerp en de juridische en technische complexiteit ervan, wenst de Commissie de Raad en het Europees Parlement te informeren over de stand van zaken en een debat op gang te brengen. De Commissie vindt dat een dergelijk debat moet worden gevoerd voordat zij op basis van een effectbeoordeling met concrete voorstellen komt.

Deze mededeling loopt dan ook niet vooruit op het voorstel dat de Commissie zal indienen. Elk toekomstig voorstel zal zijn gebaseerd op de hierboven bedoelde discussies en op de effectbeoordeling, die zal voortkomen uit een studie waartoe de Commissie in de tweede helft van 2010 opdracht heeft gegeven. Omdat een wetgevingsvoorstel belangrijke gevolgen kan hebben voor de grondrechten, en met name voor de gegevensbescherming, zal in de

---

1 PB L 195 van 27.7.2010, blz. 5.
2 Besluit van de Raad van 13 juli 2010, PB L 195 van 27.7.2010, blz. 3.
3 Zie bijvoorbeeld Resolutie P7_TA(2010)0143 en de toelichting bij Aanbeveling A7-0224/2010.
4 COM(2010) 673 definitief van 22.11.2010. Zie actie 2 in het kader van doelstelling 2, blz. 9.

effectbeoordeling in het bijzonder aandacht worden besteed aan de noodzaak en de evenredigheid van de maatregelen die de Commissie voorstelt. Daarbij zal de Commissie de richtsnoeren volgen die worden aangereikt in haar mededeling over de strategie voor de tenuitvoerlegging van het Handvest van de grondrechten[5].

Daarnaast zal de effectbeoordeling de nodige technische achtergrondinformatie verschaffen, alsmede een uitvoerige beoordeling van alle beschikbare opties. Deze punten zijn al besproken met vele belanghebbenden, zoals de autoriteiten van de lidstaten, gegevensbeschermingsautoriteiten, Europol en de aangewezen verstrekker. De definitieve resultaten van de hierboven bedoelde studie zijn pas eind dit jaar beschikbaar. Ter voorbereiding van de effectbeoordeling heeft de Europese Commissie drie bijeenkomsten van deskundigen gehouden met dezelfde belanghebbenden en met de Amerikaanse autoriteiten die betrokken zijn bij de uitvoering van het TFTP. De opties die in deze mededeling worden besproken, zijn gebaseerd op de eerste resultaten van de studie en op de discussies in deze bijeenkomsten.

2. DOEL VAN EEN EU-SYSTEEM VOOR HET TRACEREN VAN TERRORISMEFINANCIERING

Er zijn twee hoofdredenen voor het opzetten van een EU-systeem voor het traceren van terrorismefinanciering (TFTS):

- het systeem moet een doeltreffende bijdrage leveren aan de strijd tegen terrorisme en de financiering daarvan binnen de Europese Unie;

- het systeem moet ertoe leiden dat er minder persoonsgegevens worden doorgegeven aan derde landen. Het systeem moet het mogelijk maken de gegevens die nodig zijn om het systeem toe te passen, te verwerken op EU-grondgebied, met inachtneming van de EU-gegevensbeschermingsbeginselen en -regelgeving.

In de Verenigde Staten is gebleken dat het Programma voor het traceren van terrorismefinanciering (TFTP) een belangrijke meerwaarde biedt bij de bestrijding van terrorisme en de financiering daarvan, niet alleen voor de Amerikaanse autoriteiten, maar ook voor de autoriteiten van de lidstaten van de Europese Unie en voor die van derde landen. De recente evaluatie van de EU-VS TFTP-overeenkomst[6] heeft uitgewezen dat sinds de invoering van het TFTP in de VS ruim 2 500 verslagen zijn uitgewisseld met de autoriteiten van derde landen, waarvan de overgrote meerderheid (1 700) met de Europese Unie. De doeltreffendheid van het Amerikaanse programma en de betekenis ervan voor de bestrijding van terrorisme en de financiering van terrorisme worden ook bevestigd in twee verslagen van rechter Bruguière, die in 2008 door de Europese Commissie werd aangesteld om het programma te evalueren. De uit het TFTP afkomstige informatie die aan de EU-autoriteiten werd verstrekt, bevatte belangrijke aanwijzingen met betrekking tot een aantal (pogingen tot) zware terreuraanslagen, zoals die in Madrid en Londen, de plannen om in 2006 trans-Atlantische vluchten neer te halen met behulp van vloeibare explosieven, en de verijdelde aanslag op Amerikaanse doelen in Duitsland in 2007. Het evaluatieteam van de EU kwam ook tot de conclusie dat er overtuigende aanwijzingen waren dat het TFTP een meerwaarde biedt

[5] COM(2010) 573 definitief van 19.10.2010.
[6] SEC(2011) 438 definitief van 30.3.2011.

bij de bestrijding van terrorisme en terrorismefinanciering. Op grond van deze ervaringen kan worden aangenomen dat een EU-TFTS ook een duidelijke toegevoegde waarde biedt voor de inspanningen van de EU en de lidstaten om terrorisme en de financiering ervan te bestrijden.

Hoewel de doeltreffendheid van het Amerikaanse TFTP voor de bestrijding van terrorisme en terrorismefinanciering buiten kijf staat, zijn er wel ernstige bezwaren gerezen met betrekking tot de gevolgen ervan voor de grondrechten van de burgers. Deze bezwaren hebben voornamelijk betrekking op het feit dat de toepassing van de EU-VS TFTP-overeenkomst leidt tot de verstrekking van grote hoeveelheden gegevens aan de Amerikaanse autoriteiten, terwijl verreweg de meeste van die gegevens betrekking hebben op burgers die niets met terrorisme of terrorismefinanciering te maken hebben. De gegevens worden "in bulk" verstrekt (op basis van relevante gegevenscategorieën) in plaats van afzonderlijk (in antwoord op een verzoek betreffende een of meer personen), omdat de verstrekker van de gegevens technisch niet in staat is gegevens over afzonderlijke personen te verstrekken. Bovendien zou de verstrekker, om geïndividualiseerde gegevens te kunnen verstrekken, over een specifieke zoek- en analysefunctie moeten beschikken die niet nodig is voor zijn bedrijfsvoering en die aanzienlijke kosten met zich zou brengen. Tevens zou het opvragen van geïndividualiseerde gegevens betekenen dat de verstrekker zou weten naar welke personen een onderzoek wordt ingesteld in verband met terrorisme en mogelijke financiële banden met terrorisme. Dit zou gevolgen kunnen hebben voor de doeltreffendheid van dergelijke onderzoeken.

Als tegenwicht voor de verstrekking van gegevens in bulk zijn waarborgen ingebouwd die ervoor moeten zorgen dat er geen misbruik van de gegevens kan worden gemaakt; zo mogen de verstrekte gegevens uitsluitend worden doorzocht en gebruikt ten behoeve van de bestrijding van terrorisme en de financiering van terrorisme. Uit de recente evaluatie van de EU-VS TFTP-overeenkomst is gebleken dat deze waarborgen inderdaad volgens de overeenkomst worden toegepast.

Niettemin zijn sommigen van oordeel dat het verstrekken van dergelijke grote hoeveelheden persoonsgegevens aan een derde land een ongerechtvaardigde inbreuk op de grondrechten van de burgers vormt, afgezet tegen de noodzaak en de evenredigheid ervan. Daarom heeft de Raad de Commissie verzocht voorstellen in te dienen voor een systeem "voor het extraheren van gegevens op het EU-grondgebied"; zo kan ervoor worden gezorgd dat de verwerking van de gegevens gebeurt in overeenstemming met de EU-gegevensbeschermingsregels en -beginselen en met het EU-Handvest van de grondrechten. In dit verband moet worden opgemerkt dat het verzamelen en verwerken van financiële gegevens door overheidsinstanties het recht op de bescherming van persoonsgegevens, dat is verankerd in artikel 16 VWEU en artikel 8 van het Handvest, ondermijnt.

Krachtens artikel 52, lid 1, van het Handvest moeten beperkingen van deze grondrechten met het oog op de voorspelbaarheid met de nodige nauwkeurigheid en duidelijkheid bij wet worden gesteld en de wezenlijke inhoud van die rechten eerbiedigen. De beperkingen moeten noodzakelijk en evenredig zijn om een door de Unie erkende legitieme doelstelling te verwezenlijken. Deze beginselen moeten dan ook niet alleen worden meegewogen bij de beslissing al dan niet een EU-TFTS op te zetten, er moet ook rekening mee worden gehouden bij het beoordelen van de verschillende opties voor de toepassing van het systeem. Deze beginselen zijn dus van invloed op de keuzes die moeten worden gemaakt ten aanzien van het toepassingsgebied van het systeem, de toepasselijke bewaartermijnen, het recht op toegang tot en verwijdering van gegevens, enz. Deze punten worden niet uitvoerig behandeld in deze mededeling. Zij moeten grondig worden geanalyseerd in de effectbeoordeling.

Vanzelfsprekend zou de eventuele invoering van een systeem voor het extraheren van de gegevens op EU-grondgebied consequenties hebben voor de bestaande EU-VS TFTP-overeenkomst, zoals wordt erkend in artikel 11, lid 3, van de overeenkomst, waarin wordt bepaald dat aangezien de totstandbrenging van een EU-systeem de context van deze overeenkomst ingrijpend zou kunnen veranderen, de partijen overleg moeten plegen om te bepalen of de overeenkomst moet worden aangepast indien de Europese Unie besluit een dergelijk systeem in te voeren. Alle opties hebben derhalve ook gevolgen voor de toekomstige toepassing en eventuele aanpassing van de bestaande EU-VS TFTP-overeenkomst.

3. BELANGRIJKSTE FUNCTIES VAN EEN EU-SYSTEEM VOOR HET TRACEREN VAN TERRORISMEFINANCIERING

Wat duidelijk naar voren kwam bij de besprekingen met belanghebbenden is dat verreweg de meesten van hen vinden dat als er een EU-systeem voor het traceren van terrorismefinanciering (EU-TFTS) wordt opgezet, dit moet gebeuren in het belang van de veiligheid van de EU-burgers. Het systeem moet niet alleen worden ingevoerd om de Amerikaanse autoriteiten de gewenste informatie te verschaffen; de autoriteiten van de lidstaten hebben ook echt belang bij een dergelijk systeem. Deze benadering betekent ook dat het Amerikaanse TFTP weliswaar als uitgangspunt kan dienen voor hoe een dergelijk systeem kan worden opgezet, maar dat niet alle eigenschappen ervan hoeven te worden overgenomen in een soortgelijk Europees systeem. Bij het opzetten van een EU-systeem moet bovendien rekening worden gehouden met het specifieke juridische en administratieve EU-kader, waaronder de toepasselijke grondrechten, zoals hierboven reeds werd opgemerkt.

Voor elk systeem dat is bedoeld voor het traceren van terrorismefinanciering en dat aan de hierboven gestelde doelen moet beantwoorden, geldt echter dat het de volgende functies moet kunnen vervullen:

- het opstellen en afgeven van (juridisch geldige) verzoeken aan de aangewezen verstrekker(s) van diensten inzake financieel berichtenverkeer om de onbewerkte gegevens te verstrekken aan (een) geautoriseerde ontvanger(s). Dit houdt in dat moet worden bepaald welke categorie berichten moet wordt opgevraagd en hoe vaak dergelijke berichten moeten worden gezonden, en dat hierover contact moet worden onderhouden met de verstrekkers;

- het toezien op en autoriseren van verzoeken aan de aangewezen verstrekker(s) om dergelijke onbewerkte gegevens. Dit houdt in dat moet worden nagegaan of bij het verzoek om gegevens de toepasselijke beperkingen in acht zijn genomen;

- het ontvangen en opslaan (verwerken) van de onbewerkte gegevens van de aangewezen verstrekker(s), met behulp van een systeem voor de fysieke en elektronische beveiliging van de gegevens;

- het daadwerkelijk doorzoeken van de verstrekte gegevens, overeenkomstig het toepasselijke juridische kader, op verzoek van de autoriteiten van de lidstaten, de VS of andere derde landen op basis van duidelijk omschreven voorwaarden en waarborgen, of op eigen initiatief van de met de verwerking van de gegevens belaste autoriteit(en);

- het toezien op en autoriseren van het doorzoeken van de verstrekte gegevens;

- het analyseren van de resultaten van de zoekopdrachten, door deze resultaten te combineren met andere beschikbare gegevens of inlichtingen;

- het doorgeven van de resultaten van de zoekopdrachten (zonder nadere analyse) of de resultaten van de analyses aan de geautoriseerde ontvangers;

- het toepassen van een degelijke gegevensbeschermingsregeling, met bewaartermijnen, registratieverplichtingen, en het behandelen van verzoeken om toegang, correctie en verwijdering, enz.

Deze basisfuncties moeten worden geregeld bij daarop toegesneden rechtsinstrumenten op EU-niveau, op nationaal niveau, of op beide niveaus, afhankelijk van de optie die wordt gekozen.

4. UITGANGSPUNTEN BIJ HET AFWEGEN VAN DE VERSCHILLENDE OPTIES

Behalve door de hierboven beschreven functies zal de keuze tussen de beschikbare opties voor een groot deel worden bepaald door de vraag in hoeverre een optie beantwoordt aan bepaalde hieronder beschreven basisvereisten; dit wordt momenteel getoetst in het kader van de effectbeoordeling.

4.1. Doeltreffendheid

De verwachte doeltreffendheid van de verschillende opties ten aanzien van het hoofddoel, de bestrijding van terrorisme en terrorismefinanciering, is van doorslaggevend belang. Vanuit dit oogpunt verdienen opties die de mogelijkheden voor gegevensuitwisseling en analyse op internationaal niveau vergroten, de voorkeur, omdat uitwisseling en analyse de doeltreffendheid vergroten en meer toegevoegde waarde bieden. Vooral de keuze van de organisatie(s) die wordt of worden belast met de analyse van de gegevens en het verstrekken van de resultaten daarvan aan de bevoegde autoriteiten zal van groot belang zijn voor de algemene doeltreffendheid van het systeem en voor de hoeveelheid gegevens die zal worden doorgegeven. Niettemin moeten de lidstaten, net als nu, volledig kunnen blijven bepalen of hun informatie of inlichtingen met andere autoriteiten mogen worden uitgewisseld.

4.2. Gegevensbescherming

Internationale uitwisseling en analyse van informatie en inlichtingen kan alleen plaatsvinden binnen een degelijk en goed ontwikkeld kader voor gegevensbescherming. De effectiviteit van een dergelijk kader wordt niet alleen bepaald door de toepasselijke regelgeving, die betrokkenen in staat stelt hun rechten, zoals het recht op een voorziening in rechte, uit te oefenen, maar ook door de beschikbaarheid van ervaren personeel, zoals een onafhankelijke gegevensbeschermingsambtenaar en een onafhankelijke en ervaren toezichthoudende autoriteit voor gegevensbescherming. Sommige organisaties die betrokken zouden kunnen worden bij de eventuele invoering van een EU-TFTS beschikken al over dergelijke structuren, terwijl die voor andere nog in het leven zouden moeten worden geroepen. De gegevensbeschermingsaspecten van elk van de verschillende opties moeten dan ook zorgvuldig worden getoetst aan de algemene beginselen betreffende de eerbiediging van de in punt 2 van deze mededeling genoemde grondrechten.

4.3. Gegevensbeveiliging

Degelijke gegevensbeschermingsregels moeten hand in hand gaan met de allernieuwste infrastructuur en technologie op het gebied van gegevensbeveiliging. Uit overwegingen van gegevensbeveiliging zou het aantal plaatsen waar de verstrekte gegevens kunnen worden verwerkt, moeten worden beperkt, evenals de toegang tot de gegevens van buitenaf. De veiligste oplossing zou opslag op een enkele locatie zijn, zonder toegang van buitenaf. De meeste organisaties die een rol zouden kunnen spelen bij het toepassen van het TFTS werken al met beveiligde gegevensverwerking, maar zij hebben niet allemaal de capaciteit om gegevens te verwerken die hoger zijn gerubriceerd dan "EU-restricted".

4.4. Opslag van gegevens

Gegevens kunnen op nationaal of op EU-niveau worden opgeslagen. Op EU-niveau zouden de gegevens kunnen worden opgeslagen bij Europol of bij een ander EU-orgaan, zoals het agentschap voor het operationele beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (IT-agentschap)[7], dat momenteel wordt opgericht. Daar de opslag van gegevens onlosmakelijk is verbonden met de gegevensbeschermings- en gegevensbeveiligingsproblematiek, moet de keuze van de organisatie die wordt belast met de opslag van de gegevens nauw verband houden met de gegevensbeschermings- en -beveiligingssystemen die deze organisaties te bieden hebben.

4.5. Gebruikmaken van bestaande structuren en instrumenten

Bij alle opties moet zo veel mogelijk gebruik worden gemaakt van bestaande structuren. Dit drukt de kosten en biedt de mogelijkheid nuttig gebruik te maken van opgedane ervaringen en bestaande infrastructuur. Er moet goed op worden gelet dat de nieuwe taken die aan een bestaande organisatie worden toegewezen, passen bij het bestaande mandaat van die organisatie. Zo zou kunnen worden overwogen Europol, Eurojust of nationale justitiële autoriteiten te belasten met het controleren en autoriseren van verzoeken aan de aangewezen verstrekker(s) om gegevens te verstrekken.

4.6. Samenwerking tussen verantwoordelijke autoriteiten

De hieronder beschreven opties verschillen wat betreft de mate van samenwerking en uitwisseling van informatie en inlichtingen tussen nationale autoriteiten en tussen nationale en Europese autoriteiten. De lidstaten hebben uiteenlopende manieren ontwikkeld waarop hun nationale autoriteiten samenwerken bij de bestrijding van terrorisme, en bij maatregelen op Europees niveau moet rekening worden gehouden met de beperkingen die in artikel 72 VWEU worden gesteld in verband met de verantwoordelijkheid van de lidstaten voor de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid. Een EU-TFTS moet de lidstaten dan ook grote zeggenschap bieden over de informatie en inlichtingen die zij in het kader van een dergelijk systeem willen uitwisselen. De hieronder genoemde organisaties hebben verschillende werkwijzen op dit gebied ontwikkeld, waarvan sommige direct in het nieuwe systeem zouden kunnen worden toegepast.

---

[7] COM(2010) 93 definitief van 19.3.2010.

4.7. Eerste algemene overzicht van de mogelijke financiële consequenties van de verschillende opties

De totale kosten van het opzetten van een EU-TFTS en de verdeling daarvan tussen de EU en de lidstaten hangen voor een groot deel af van de beleidsoptie die wordt gekozen. De kosten omvatten in elk geval:

- de kosten in verband met de beveiligde doorgifte en opslag van de gegevens die worden ontvangen van de aangewezen verstrekker(s);
- de ontwikkelings- en onderhoudskosten van de sofware die nodig is om de zoekopdrachten uit te voeren en de resultaten daarvan te leveren;
- de kosten van het doorgeven van de resultaten van de zoekopdrachten of de analyses aan de geautoriseerde ontvangers;
- personeelskosten voor het personeel dat de zoekopdrachten uitvoert, de analyses verricht en de resultaten verspreidt;
- personeelskosten voor het personeel dat zich bezighoudt met toezicht en audit;
- personeelskosten voor het personeel dat zich bezighoudt met gegevensbescherming en rechten van de burgers.

Hoewel er op dit moment nog geen gedetailleerde kostenramingen beschikbaar zijn, wijzen de eerste berekeningen erop dat bij de zuivere EU-aanpak en alle verschillende mengvormen die hieronder worden besproken, de aanloopkosten tussen de 33 en 47 miljoen EUR zouden bedragen, en de jaarlijkse exploitatiekosten 7 à 11 miljoen EUR. In punt 6 van deze mededeling worden verschillende opties beschreven. Optie 3 is de duurste optie, met 43 miljoen EUR aanloopkosten voor de EU en 3,7 miljoen EUR voor de lidstaten (samen), en 4,2 miljoen EUR jaarlijkse exploitatiekosten voor de EU en 6,8 miljoen EUR voor de lidstaten (samen). Optie 2 is de goedkoopste optie, met 33 miljoen EUR aanloopkosten voor de EU en daarnaast aan jaarlijkse exploitatiekosten 3,5 miljoen EUR voor de EU en 3,3 miljoen EUR voor de lidstaten (samen). Optie 1 kost aan aanloopkosten 40,5 miljoen EUR voor de EU en aan jaarlijkse exploitatiekosten 4 miljoen EUR voor de EU en 5 miljoen EUR voor de lidstaten (samen). Deze kosten vallen uiteraard lager uit als gebruik kan worden gemaakt van personeel van bestaande organisaties, of van bestaande infrastructuur en soft- en hardware. Voor een puur nationaal systeem zouden de aanloop- en exploitatiekosten veel hoger liggen (390 miljoen EUR aanloopkosten, 37 miljoen jaarlijkse exploitatiekosten), omdat alle lidstaten zwaarbeveiligde gegevensverwerkingssystemen zouden moeten invoeren en personeel zouden moeten aannemen om het systeem te bedienen.

Dit zijn voorlopige bedragen, die nader moeten worden bekeken in het licht van de resultaten van de effectbeoordeling.

5. AANDACHTSPUNTEN

Los van de keuze tussen de verschillende opties voor de opzet en werking van een EU-TFTS, moet een aantal belangrijke vragen worden beantwoord over de reikwijdte van een dergelijk systeem. Deze worden hieronder besproken.

5.1. Terrorisme en terrorismefinanciering of breder?

Toegang tot gegevens betreffende het financiële berichtenverkeer is niet alleen nuttig voor de bestrijding van terrorisme en terrorismefinanciering. Het lijdt geen twijfel dat dit ook een nuttig instrument zou zijn voor de bestrijding van andere vormen van zware criminaliteit, met name georganiseerde criminaliteit en het witwassen van geld. Binnen het kader van de EU-VS TFTP-overeenkomst is met het oog op de evenredigheid het gebruik van de gegevens echter strikt beperkt tot de bestrijding van terrorisme en terrorismefinanciering. De besprekingen die tot nu toe zijn gevoerd, wijzen erop dat er brede consensus bestaat dat uit dezelfde evenredigheidsoverwegingen voor een vergelijkbaar Europees systeem het toepassingsgebied op dezelfde manier moet worden afgebakend, gezien de overwegingen betreffende de eerbiediging van de grondrechten die in punt 2 van deze mededeling aan de orde zijn gekomen.

5.2. Meer dan één verstrekker?

In het kader van de EU-VS TFTP-overeenkomst kunnen slechts van één aanbieder van diensten op het gebied van internationaal financieel berichtenverkeer gegevens worden opgevraagd. Hoewel deze verstrekker verreweg de belangrijkste aanbieder van dergelijke diensten ter wereld is, zijn er ook andere verstrekkers actief op de markt. Met het oog op efficiëntie en gelijke voorwaarden voor alle marktdeelnemers moet worden gedacht aan een systeem dat van toepassing is op alle aanbieders van diensten op het gebied van het internationale financiële berichtenverkeer. In elk geval moet bij de keuze tussen de beschikbare opties ook worden gekeken naar de administratieve last voor de ondernemingen die dergelijke diensten aanbieden.

5.3. Alleen internationaal of ook nationaal betalingsverkeer?

In het kader van de EU-VS TFTP-overeenkomst kunnen alleen gegevens worden opgevraagd van aanbieders van diensten op het gebied van het internationale financiële berichtenverkeer, d.w.z. diensten voor het verrichten van grensoverschrijdende transacties, waaronder die tussen de EU-lidstaten, maar met uitzondering van gegevens betreffende het financiële berichtenverkeer die betrekking hebben op de eengemaakte eurobetalingsruimte (SEPA). Het is de vraag of een EU-TFTS het financiële berichtenverkeer tussen de lidstaten moet omvatten of dat het beperkt moet blijven tot internationale diensten op het gebied van het financiële berichtenverkeer. Zuiver nationale diensten voor financieel berichtenverkeer (die alleen worden gebruikt voor nationale financiële transacties) vallen momenteel buiten de werkingssfeer van de EU-VS TFTP-overeenkomst. Toegang tot het nationale financiële berichtenverkeer zou van belang zijn voor de bestrijding van terrorisme en andere vormen van criminaliteit. Maar los van de vraag of de toegang tot gegevens over zuiver nationale transacties wel op Europees niveau zou moeten worden geregeld, blijkt uit de eerste besprekingen dat deze toegang over het algemeen als onevenredig wordt beschouwd en daarom buiten een EU-systeem zou moeten vallen.

5.4. Welke gegevens betreffende het financiële berichtenverkeer moeten worden verstrekt?

In het internationale bankwezen worden veel verschillende soorten gegevens over het financiële berichtenverkeer gebruikt. De EU-VS TFTP-overeenkomst heeft slechts betrekking op één specifiek soort gegevens. Toegang tot andere gegevens betreffende het financiële berichtenverkeer zou van belang zijn voor de bestrijding van terrorisme en

terrorismefinanciering, en mogelijk ook andere vormen van criminaliteit. Ook in dit geval lijkt het soort berichtenverkeer waarop het systeem betrekking heeft, met het oog op de evenredigheid en de eerbiediging van de grondrechten van de burgers echter te moeten worden beperkt. Op dit technische aspect zal nader worden ingegaan in de effectbeoordeling.

6. OPTIES VOOR EEN EU-TFTS

De opties die hieronder worden beschreven, worden momenteel door de Commissie onderzocht in het kader van de lopende effectbeoordeling. Dat wil niet zeggen dat er geen andere opties mogelijk zijn en de beschrijving hieronder loopt ook niet vooruit op de uiteindelijke effectbeoordeling of op de keuze die de Commissie op basis daarvan zou maken.

Een van de opties die altijd wordt bekeken bij nieuwe initiatieven en de bijbehorende effectbeoordeling is de optie om de status quo te handhaven; in dit geval zou dat betekenen dat de EU-VS TFTP-overeenkomst van kracht blijft en dat er geen voorstel wordt gedaan voor een EU-TFTS. Met deze optie zou niet worden ingegaan op het in punt 1 van deze mededeling bedoelde verzoek van de Raad en het Parlement aan de Commissie om met een voorstel te komen voor "een juridisch en technisch kader voor het extraheren van gegevens op het EU-grondgebied". Bovendien zou deze optie er niet toe leiden dat er minder persoonsgegevens worden doorgegeven aan derde landen, noch dat de gegevens op EU-grondgebied worden verwerkt overeenkomstig de EU-gegevensbeschermingsbeginselen en -wetgeving. De overige opties bieden alle de mogelijkheid om een EU-TFTS in te voeren.

In theorie kunnen alle basisfuncties van een EU-TFTS zoals die in punt 3 van deze mededeling zijn beschreven, hetzij op EU-niveau hetzij op nationaal niveau worden uitgevoerd. De functies kunnen ook aan een of meer verschillende organisaties worden toegewezen, in overeenstemming met hun bestaande verantwoordelijkheden, of aan nieuwe organisaties die speciaal zouden worden opgericht om deze functies uit te voeren. Dat zouden Europese of nationale organisaties kunnen zijn. Dit houdt – eveneens in theorie – in dat een zuiver Europese aanpak mogelijk is, waarbij alle basisfuncties worden toevertrouwd aan organisaties op EU-niveau, maar ook een zuiver nationale aanpak, waarbij alle functies op nationaal niveau worden uitgeoefend. Wat ook niet uit het oog moet worden verloren, is dat de keuze voor een centraal, decentraal of mengvormsysteem in dit geval niet noodzakelijkerwijs dezelfde hoeft te zijn als de keuze die is gemaakt ten aanzien van andere initiatieven op het gebied van gegevensverwerking ter bestrijding van terrorisme en georganiseerde criminaliteit – elk initiatief op dit gebied moet op zijn eigen kenmerken worden beoordeeld.

Zowel een zuiver centrale als een zuiver nationale aanpak heeft grote nadelen. Zo zou een exclusief Europese aanpak waarschijnlijk te veraf staan van de rechtshandhavings- en inlichtingeninstanties en -werkwijzen van de lidstaten en daarom niet erg effectief zijn. Zonder medewerking van de nationale autoriteiten die belast zijn met deze zaken, zou het welhaast onmogelijk zijn om nauwkeurig te bepalen welke categorieën gegevens moeten worden opgevraagd van de aangewezen verstrekker(s). Het systeem zou ook veel minder zinvol zijn als de database alleen zou kunnen worden doorzocht op basis van de inlichtingen die op EU-niveau beschikbaar zijn: bij de huidige stand van EU-integratie zijn deze inlichtingen grotendeels uitsluitend op nationaal niveau beschikbaar. Bovendien zouden de lidstaten waarschijnlijk niet instemmen met een zuiver centrale aanpak, omdat die geen meerwaarde zou bieden voor hun eigen inspanningen om terrorisme en terrorismefinanciering

te bestrijden. Tijdens de besprekingen hebben de lidstaten ook aangegeven dat deze optie om juridische en operationele redenen politiek moeilijk aanvaardbaar zou zijn.

Het andere uiterste, een zuiver nationale aanpak, bergt het gevaar in zich dat de lidstaten het systeem op uiteenlopende wijze ten uitvoer leggen en verhoogt het risico dat de gegevensbeveiliging tekortschiet, omdat er 27 versies van de verstrekte gegevens nodig zijn. Een zuiver nationale aanpak ondermijnt ook de toepassing van een geharmoniseerd gegevensbeschermingskader en een geharmoniseerde aanpak van (het toezicht op) andere noodzakelijke restricties, zoals de doelbeperking tot terrorisme en terrorismefinanciering. Tevens is bij een puur nationale aanpak onduidelijk welke lidstaat verantwoordelijk is voor het behandelen van verzoeken van derde landen; ook het voordeel van een analyse van de resultaten op Europees niveau zou verloren gaan. Daar komt nog bij dat, zoals hierboven al werd opgemerkt, de kosten bij deze optie veel hoger zouden uitvallen, omdat alle lidstaten zwaar beveiligde gegevensverwerkingssystemen zouden moeten invoeren en personeel zouden moeten aannemen om het systeem te bedienen.

Bij de voorbereidende werkzaamheden met de belanghebbenden bleek dan ook al snel dat er geen steun was voor de opties aan beide uiteinden van het spectrum van mogelijke opties; men was het erover eens dat een mengvorm, waarbij de verschillende functies aan verschillende organisaties op EU- en op nationaal niveau worden toegewezen, de beste resultaten zou opleveren ten aanzien van de twee hoofddoelstellingen. Hoewel deze consensus het gemakkelijker maakt de meest geschikte optie te kiezen, moet voor een mengvorm nog steeds een groot aantal knopen worden doorgehakt. Hieronder worden de drie mengvormen die uit de lopende voorbereidende werkzaamheden naar voren kwamen als de meest geschikte, nader omschreven; deze opties worden ook in tabelvorm weergegeven in de bijlage.

6.1. Centrale EU-TFTS-dienst voor coördinatie- en analyse (optie 1)

Bij deze optie wordt een centrale EU-TFTS-eenheid opgericht en worden de meeste taken en functies op EU-niveau uitgevoerd. Het afgeven van verzoeken om onbewerkte gegevens aan de aangewezen verstrekker(s), de controle van deze verzoeken, het behandelen van zoekopdrachten en het verrichten daarvan, het beheren van de zoekresultaten en het doorgeven van verslagen aan degenen die de zoekopdracht hebben gegeven, zou allemaal op EU-niveau gebeuren. Het opstellen van verzoeken aan de aangewezen verstrekker(s) zou echter kunnen gebeuren in overleg met de verantwoordelijke autoriteiten van de lidstaten, en de lidstaten zouden er ook voor kunnen kiezen hun eigen analisten af te vaardigen naar de centrale eenheid, zodat zij kunnen deelnemen aan het uitvoeren van zoekopdrachten. Anders dan bij de zuiver centrale optie, zouden de lidstaten kunnen vragen zoekopdrachten namens hen te verrichten, zoals nu ook kan in het kader van de VS TFTP, of zoekopdrachten door hun eigen analisten te laten verrichten.

De lidstaten zouden informatie moeten uitwisselen met de centrale EU-TFTS-eenheid om het verzoek te "onderbouwen" en aan te tonen dat er een verband is met terrorisme, voordat een zoekopdracht zou kunnen worden uitgevoerd, of zij zouden hun verzoek van tevoren moeten laten autoriseren door de nationale autoriteiten. Deze nationale autoriteiten zouden bijvoorbeeld kunnen worden vertegenwoordigd door openbare aanklagers of onderzoeksrechters die zijn belast met terrorismebestrijding: als zij een bepaalde zoekopdracht in de verstrekte gegevens zouden autoriseren, zou de centrale EU-TFTS-eenheid deze zoekopdracht zonder verdere verificatie kunnen uitvoeren. In deze opzet zouden verder geen inlichtingen aan de centrale EU-TFTS-eenheid hoeven te worden verstrekt. De

centrale EU-TFTS-eenheid zou de resultaten en de analyse daarvan doorgeven en ook spontaan informatie kunnen verstrekken. De VS en andere derde landen zouden ook een verzoek om een zoekopdracht moeten indienen volgens een vergelijkbare procedure.

Het toezicht op de naleving van de waarborgen en de controle zouden ook centraal gebeuren, eventueel onder toezicht van externe belanghebbenden, bijvoorbeeld vertegenwoordigers van de aangewezen verstrekker(s) en degenen die als onafhankelijk toezichthouder zijn aangewezen. Gegevenbescherming, -integriteit en -beveiliging zouden ook op centraal niveau worden gewaarborgd.

De belangrijkste organen die bij het systeem zouden kunnen worden betrokken, zijn Europol en Eurojust. De taken van Europol en Eurojust zouden moeten stroken met hun mandaat dat is vastgelegd in het Verdrag betreffende de werking van de Europese Unie (VWEU). Tevens moet worden vastgesteld in hoeverre de rechtsinstrumenten waarin de werking van beide organen is geregeld, moeten worden gewijzigd. Als Europol wordt gekozen als de centrale EU-TFTS-autoriteit moet het ook verzoeken behandelen van betrokkenen die vragen om toegang tot of om rectificatie of afscherming van hun gegevens, en daarbij moeten handelen in overeenstemming met het bestaande juridische kader en de bestaande gegevensbeschermingsregels. De centrale EU-TFTS-eenheid zou haar rol moeten vervullen overeenkomstig het bestaande rechtskader, en herzieningen en beroepen zouden ook worden behandeld volgens de bestaande juridische voorschriften. Op nationaal niveau zouden de rechtshandhavingsautoriteiten worden belast met het controleren en autoriseren van verzoeken om zoekopdrachten. Het is mogelijk om nieuwe nationale organen op te richten, maar op basis van het subsidiariteitsbeginsel moet deze keuze aan de lidstaten worden overgelaten[8].

6.2. Centrale EU-TFTS-dienst voor gegevensextractie (optie 2)

Evenals bij de eerste optie wordt bij deze optie een centrale EU-TFTS-eenheid opgezet die wordt belast met het afgeven van verzoeken om onbewerkte gegevens aan de aangewezen verstrekker(s), de controle van deze verzoeken, het uitvoeren van zoekopdrachten en het behandelen van verzoeken om zoekopdrachten. Maar bij deze optie zou de centrale EU-TFTS-eenheid niet de bevoegdheid hebben om de zoekresultaten te analyseren en te vergelijken met andere beschikbare informatie of inlichtingen, indien de zoekopdracht wordt verricht op verzoek van de autoriteiten van een lidstaat; in dergelijke gevallen zou de rol van de centrale eenheid beperkt blijven tot het ordenen en verspreiden van de zoekresultaten.

Evenals bij optie 1 zouden verzoeken om onbewerkte gegevens aan de aangewezen verstrekker(s) worden afgegeven in nauwe samenwerking met de lidstaten, die hun specifieke behoeften kenbaar kunnen maken bij de centrale TFTS-eenheid, die deze zou analyseren en het verzoek op basis daarvan zou kunnen formuleren.

De autoriteiten van de lidstaten kunnen verzoeken indienen om namens hen zoekopdrachten te verrichten. In hoeverre dergelijke verzoeken gegrond zijn en verband houden met terrorisme zou worden gecontroleerd en gevalideerd op nationaal niveau. De centrale EU-TFTS-eenheid zou de zoekopdracht uitvoeren en de resultaten op geordende wijze aan de lidstaten doorgeven. De autoriteiten van de lidstaten zouden de enige zijn die de zoekopdrachten analyseren, en zij zouden ook spontaan informatie kunnen verstrekken.

---

[8] Op dit moment is nog niet duidelijk wat de gevolgen zijn voor de begroting van de EU-organen die mogelijk een rol gaan spelen bij de tenuitvoerlegging van het systeem.

De centrale EU-TFTS-eenheid zou worden belast met het uitvoeren van zoekopdrachten en het analyseren van de resultaten namens de EU-instellingen, de VS en andere derde landen. Zij zou ook spontaan informatie kunnen verstrekken.

Evenals bij de vorige optie zou het toezicht op de naleving van de waarborgen en de controle centraal gebeuren, eventueel onder toezicht van externe belanghebbenden, bijvoorbeeld vertegenwoordigers van de aangewezen verstrekker(s) en degenen die als onafhankelijk toezichthouder zijn aangewezen. Gegevenbescherming, –integriteit en –beveiliging zouden ook op centraal niveau worden gewaarborgd.

En ook de belangrijkste organen die bij het systeem zouden kunnen worden betrokken, Europol en Eurojust, zouden dezelfde zijn als bij de vorige optie. Op nationaal niveau zouden de rechtshandhavingsinstanties of de inlichtingendiensten een belangrijke rol spelen. Evenals bij de vorige optie zou de beslissing over het al dan niet oprichten van nieuwe organen, op basis van het subsidiariteitsbeginsel worden overgelaten aan de lidstaten. Europol en/of de nationale eenheden zouden verzoeken behandelen van EU-burgers die vragen om toegang tot of om rectificatie of verwijdering van hun gegevens, in samenwerking met nationale gegevensbeschermingsautoriteiten en het gemeenschappelijke controleorgaan van Europol. Herzieningen en beroepen zouden worden behandeld volgens de toepasselijke wettelijke voorschriften op nationaal of op EU-niveau[9].

6.3. FIE-dienst voor coördinatie (optie 3)

Bij deze optie zou een versterkt FIE-platform worden opgericht, bestaande uit alle FIE's van de lidstaten. De ad-hocautoriteit op EU-niveau zou verzoeken om onbewerkte gegevens aan de aangewezen verstrekker(s) afgeven door de behoeften van de FIE's in een enkel verzoek onder te brengen, dat ook zou worden gecontroleerd en toegestaan op centraal niveau.

Iedere FIE zou verantwoordelijk zijn voor het uitvoeren van zoekopdrachten en het beheren van de resultaten ervan namens de eigen lidstaat, alsook voor het verrichten van analyses en het doorsturen van verslagen aan degenen voor wie zij deze relevant acht. In hoeverre zoekopdrachten gegrond zijn en verband houden met terrorisme zou worden gecontroleerd en gevalideerd op nationaal niveau of op EU-niveau. De FIE's zouden ook verantwoordelijk zijn voor het spontaan verstrekken van informatie.

Het versterkte FIE-platform zou zoekopdrachten kunnen verrichten en de resultaten kunnen analyseren namens de EU-instellingen en andere derde landen waarmee de EU daartoe een overeenkomst heeft gesloten. Het zou ook spontaan informatie kunnen verstrekken.

Het toezicht op de naleving van de waarborgen en de controle zouden centraal gebeuren, eventueel onder toezicht van externe belanghebbenden, bijvoorbeeld vertegenwoordigers van de aangewezen verstrekker(s) en degenen die als onafhankelijk toezichthouder zijn aangewezen. Gegevenbescherming, -integriteit en -beveiliging zouden ook op centraal niveau worden gewaarborgd.

Het versterkte FIE-platform zou een formele juridische status krijgen met duidelijk omschreven taken en verantwoordelijkheden. Op nationaal niveau zouden de FIE's en de rechtshandhavingsinstanties of de inlichtingendiensten een belangrijke rol spelen.

---

[9] Zie voetnoot 8.

Een autoriteit op EU-niveau zou verzoeken van burgers om toegang tot en rectificatie of verwijdering van hun gegevens behandelen, en herzieningen en beroepen zouden worden behandeld volgens de toepasselijke wettelijke voorschriften op nationaal of op EU-niveau.

7. CONCLUSIE

Op basis van de voorbereidende werkzaamheden die de Commissie tot nu toe heeft verricht, en onverminderd de resultaten van de effectbeoordeling worden in deze mededeling de verschillende opties beschreven voor het opzetten van een "juridisch en technisch kader voor het extraheren van gegevens op het EU-grondgebied" in de context van een systeem voor het traceren van terrorismefinanciering. Uit de verschillende opties die in deze mededeling worden geschetst, blijkt dat er nog belangrijke keuzes moeten worden gemaakt en beslissingen moeten worden genomen, onder meer ten aanzien van de eerbiediging van de grondrechten, en dat er nog vele juridische, technische, organisatorische en financiële aspecten nader moeten worden behandeld in het kader van de verdere voorbereidende werkzaamheden. Gezien deze belangrijke opgaven is de Commissie van mening dat er voldoende tijd moet worden uitgetrokken voor verdere voorbereidende werkzaamheden en voor een debat met de Raad en het Parlement.

*** * ***

Bijlage: Tabel mengvormen

	Centrale EU-TFTS-dienst voor coördinatie en analyse (optie 1)	Centrale EU-TFTS-dienst voor gegevensextractie (optie 2)	FIE-dienst voor coördinatie (optie 3)
Opstellen en afgeven van verzoeken om onbewerkte gegevens.	Centrale EU-TFTS-eenheid in samenwerking met lidstaten	Centrale EU-TFTS-eenheid in samenwerking met lidstaten	Versterkt FIE-platform
Toezien op en autoriseren van verzoeken om onbewerkte gegevens	Eurojust of een ander bestaand orgaan	Eurojust of een ander bestaand orgaan	Eurojust of een ander bestaand orgaan
Ontvangst en opslag van de onbewerkte gegevens, gegevensbeveiliging	Europol of ander EU-orgaan zoals het IT-agentschap	Europol of ander EU-orgaan zoals het IT-agentschap	Europol of ander EU-orgaan, zoals het IT-agentschap
Zoekopdrachten uitvoeren op de onbewerkte gegevens	Centrale EU-TFTS-eenheid, door lidstaten afgevaardigde analisten of combinatie van beide	Centrale EU-TFTS-eenheid	FIE's, versterkt FIE-platform
Toezien op en autoriseren van het verrichten van zoekopdrachten	Onafhankelijke toezichthouders, eventueel nationale autoriteiten	Onafhankelijke toezichthouders, nationale autoriteiten	Onafhankelijke toezichthouders
Analyse van de resultaten van de zoekopdrachten	Centrale EU-TFTS-eenheid, door lidstaten afgevaardigde analisten of combinatie van beide	Nationale autoriteiten voor nationale zoekopdrachten, analisten van centrale EU-TFTS-eenheid voor zoekopdrachten van EU en derde landen	Versterkt FIE-platform, nationale FIE's
Verspreiding van de resultaten van de zoekopdrachten	Analisten van Europol of afgevaardigde analisten van de lidstaten	Nationale autoriteiten voor nationale zoekopdrachten, analisten van centrale EU-TFTS-eenheid voor zoekopdrachten van EU en derde	Versterkt FIE-platform, nationale FIE's

		landen	
Toepassing van een degelijke gegevens-beschermingsregeling	Europol of ander EU-orgaan, zoals het IT-agentschap	Europol of ander EU-orgaan, zoals het IT-agentschap	Europol of ander EU-orgaan, zoals het IT-agentschap