EUROPESE
COMMISSIE

Brussel, 25.1.2017
COM(2017) 41 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE EUROPESE RAAD EN DE RAAD

Vierde voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie

Vierde voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie

I. INLEIDING

Dit is het vierde maandelijkse verslag over de vorderingen die zijn gemaakt bij de totstandbrenging van een echte en doeltreffende Veiligheidsunie. Het heeft betrekking op de ontwikkelingen in verband met twee belangrijke pijlers: *de bestrijding van terrorisme en georganiseerde criminaliteit en van de middelen ter ondersteuning daarvan; en de verbetering van onze weerbaarheid en veerkracht tegenover die dreigingen.* In dit verslag wordt ingegaan op vier belangrijke onderwerpen: informatiesystemen en interoperabiliteit, de bescherming van zachte doelwitten, cyberdreigingen en gegevensbescherming in het kader van strafrechtelijke onderzoeken.

De aanval op de kerstmarkt van Berlijn in december heeft nogmaals gewezen op ernstige tekortkomingen in onze informatiesystemen. Die moeten dringend worden aangepakt, met name op EU-niveau, om de nationale grens- en rechtshandhavingsautoriteiten op het terrein te helpen hun veeleisende taken efficiënter uit te voeren. Dat de verschillende informatiesystemen niet onderling verbonden zijn – waardoor daders meerdere identiteiten kunnen gebruiken om onopgemerkt te circuleren, ook bij het oversteken van grenzen – en de lidstaten die informatie niet systematisch uploaden in de desbetreffende EU-databanken, zijn praktische tekortkomingen bij de implementatie die dringend moeten worden verholpen. Voorts zijn meer inspanningen nodig met betrekking tot rechtshandhavingsmaatregelen aan de grenzen en de terugkeer van personen van wie de asielaanvraag is verworpen[1].

Op het gebied van de bescherming van zachte doelwitten zal de Commissie meer vaart zetten achter haar werkzaamheden om deskundigen uit de lidstaten bijeen te brengen teneinde beste praktijken uit te wisselen en standaardrichtsnoeren vast te stellen.

De cyberdreiging waarmee de EU af te rekenen krijgt, is al breed uitgemeten in de media en dit verslag gaat in op de verschillende werkgebieden waar deze problematiek reeds aan de orde is. Hierbij gaat het zowel om preventie – door samenwerking met het bedrijfsleven om het concept van ingebouwde beveiliging (“security by design”) te bevorderen en door de uitvoering van de richtlijn betreffende de beveiliging van netwerk- en informatiesystemen – als om het stimuleren van samenwerking tussen de lidstaten en met internationale organisaties en partners om aan cyberaanvallen het hoofd te kunnen bieden op het moment dat die zich voordoen. De komende maanden zullen de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid bepalen welke maatregelen nodig zijn om te zorgen voor een doeltreffende EU-brede respons op deze dreigingen. Uitgangspunt hiervoor zal de EU-strategie voor cyberbeveiliging van 2013 zijn.

De bescherming van de persoonlijke levenssfeer en van persoonsgegevens is een grondrecht en dus een hoeksteen van elke maatregel die naar een echte Veiligheidsunie leidt. De richtlijn inzake gegevensbescherming op politieel en strafrechtelijk gebied, die

[1] De Commissie zal de komende weken een herzien actieplan inzake terugkeer voorleggen; zie het verslag van de Commissie aan het Europees Parlement, de Europese Raad en de Raad over het operationeel maken van de Europese grens- en kustwacht (COM(2017) 42).

in april 2016 is aangenomen, garandeert een hoog gemeenschappelijk niveau van gegevensbescherming en zal daarom een vlotte uitwisseling van belangrijke gegevens tussen de rechtshandhavingsautoriteiten van de lidstaten vergemakkelijken. Daarnaast is de Commissie gestart met de herziening van de e-privacyrichtlijn als onderdeel van haar gegevenspakket; doel hiervan is de werkingssfeer van die richtlijn uit te breiden tot alle aanbieders van elektronische communicatie en de bepalingen ervan op één lijn te brengen met de algemene verordening gegevensbescherming. Het voorstel is bedoeld om ervoor te zorgen dat de privacy van de elektronische communicatie wordt gewaarborgd, maar geeft ook aan op welke gronden kan worden overwogen de werkingssfeer van de e-privacyverordening te beperken, bijv. wegens de nationale veiligheid of met het oog op een strafrechtelijk onderzoek.

II. VERSTERKING VAN INFORMATIESYSTEMEN EN INTEROPERABILITEIT

In de toespraak van voorzitter Juncker over de Staat van de Unie in september 2016 en in de conclusies van de Europese Raad van december 2016 wordt gewezen op het belang van het verhelpen van de huidige tekortkomingen op het vlak van informatiebeheer en het verbeteren van de **interoperabiliteit en interconnectie van de bestaande informatiesystemen**. Recente gebeurtenissen hebben opnieuw gewezen op de dringende noodzaak om de bestaande EU-databanken aan elkaar te koppelen, niet in de laatste plaats om de grens- en rechtshandhavingsautoriteiten op het terrein de nodige instrumenten te geven om identiteitsfraude op te sporen. Zo gebruikte de dader van de terroristische aanslag van december 2016 in Berlijn minstens 14 verschillende identiteiten en kon hij van de ene lidstaat naar de andere gaan zonder te worden opgemerkt. Het is duidelijk dat de bestaande en de toekomstige informatiesystemen van de EU gelijktijdig en met behulp van biometrische kenmerken moeten kunnen worden doorzocht om deze weg voor terroristen en criminelen af te sluiten.

De Commissie heeft de werkzaamheden op dit gebied in april 2016 gestart met haar voorstellen voor "Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid"[2]. Hierin heeft zij gewezen op tekortkomingen in de werking van de bestaande systemen, lacunes in de EU-architectuur voor gegevensbeheer, problemen met het complexe landschap van op uiteenlopende wijze beheerde informatiesystemen en een algemene versnippering als gevolg van het feit dat de bestaande systemen afzonderlijk werden opgezet en niet op elkaar zijn afgestemd. Als onderdeel van dit proces is de Commissie gestart met de **deskundigengroep op hoog niveau inzake informatiesystemen en interoperabiliteit**, waaraan EU-agentschappen, lidstaten en relevante belanghebbenden deelnemen. In het verslag van de voorzitter van 21 december 2016[3] worden de **voorlopige bevindingen** van de groep weergegeven, met als prioritaire optie de oprichting van één enkel zoekportaal waarmee nationale rechtshandhavings- en grensautoriteiten gelijktijdige zoekopdrachten kunnen verrichten in de bestaande databanken en informatiesystemen van de EU. In dat tussentijdse verslag wordt ook gewezen op het belang van de kwaliteit van de gegevens – aangezien de informatiesystemen slechts zo doeltreffend zijn als de kwaliteit en het format van de

[2] Mededeling "Krachtigere en slimmere informatiesystemen voor grenzen en veiligheid" COM(2016) 205 final.

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

daarin ingevoerde gegevens – en worden aanbevelingen gedaan om de kwaliteit van de gegevens in de EU-systemen te verbeteren door een geautomatiseerde kwaliteitscontrole van de gegevens.

De Commissie zal snel werk maken van de optie om één enkel zoekportaal op te richten en zal, samen met het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen (eu-LISA), beginnen te werken aan een portaal waarmee alle belangrijke bestaande EU-systemen tegelijk kunnen worden doorzocht. Een studie die in verband daarmee wordt uitgevoerd, moet uiterlijk in juni klaar zijn en zal dienen als basis om vóór het einde van het jaar een prototype van dat portaal te ontwerpen en te testen. De Commissie is van mening dat, parallel daarmee, ook Europol moet blijven werken aan een systeeminterface waarmee de frontlijnfunctionarissen van de lidstaten, telkens als zij hun eigen nationale systemen raadplegen, automatisch ook de databanken van Europol raadplegen.

De werkzaamheden om de informatiesystemen interoperabel te maken zijn bedoeld om een einde te maken aan de huidige versnippering binnen de EU-architectuur voor gegevensbeheer ten behoeve van grenscontroles en beveiliging, en aan de blinde vlekken die daar het gevolg van zijn. Als gegevensbanken gebruikmaken van een gemeenschappelijk register van identiteitsgegevens – zoals dat is gepland voor het voorgestelde EU-inreis/uitreissysteem en het voorgestelde Europees systeem voor reisinformatie en -autorisatie (ETIAS) – kan een persoon slechts onder één enkele identiteit in de verschillende databanken worden geregistreerd, waardoor gebruik van verschillende valse identiteiten wordt voorkomen. Als een eerste stap heeft de Commissie, zoals gesuggereerd in de voorlopige bevindingen van de groep deskundigen op hoog niveau, eu-LISA verzocht om een analyse te maken van de technische en operationele aspecten van de implementatie van een gedeelde dienst voor biometrische matching. Een dergelijke dienst maakt het mogelijk verschillende databanken met biometrische gegevens te doorzoeken, waardoor valse identiteiten die de betrokken persoon in een ander systeem gebruikt, aan het licht kunnen komen. Daarnaast zou de deskundigengroep op hoog niveau nu ook moeten beoordelen of het noodzakelijk, technisch haalbaar en evenredig is om het **gemeenschappelijke identiteitsregister** waaraan wordt gedacht voor het inreis-/uitreissysteem en ETIAS, naar andere systemen uit te breiden. Naast de biometrische gegevens die in het biometrisch matchingsysteem zouden worden opgeslagen, zou dat gemeenschappelijke identiteitsregister ook alfanumerieke identiteitsgegevens bevatten. De groep zal uiterlijk eind april 2017 haar bevindingen hierover in haar eindverslag voorleggen.

Recente beveiligingsincidenten wijzen erop dat de kwestie van de **verplichte uitwisseling van gegevens** tussen de lidstaten opnieuw moet worden aangekaart. Het voorstel van de Commissie van december 2016 tot versterking van het **Schengeninformatiesysteem** houdt – voor het eerst – de verplichting voor de lidstaten in om personen te signaleren die in verband worden gebracht met terroristische misdrijven. Het is van belang dat de medewetgevers nu werken aan een snelle aanneming van de voorgestelde maatregelen. De Commissie is bereid te onderzoeken of ook voor andere EU-databases een verplichting tot informatie-uitwisseling moet worden opgelegd.

III. BESCHERMING VAN ZACHTE DOELWITTEN TEGEN TERRORISTISCHE AANSLAGEN

De aanslag in Berlijn was de meest recente van de aanslagen die in de EU zijn gepleegd tegen zogenaamde zachte doelwitten, doorgaans civiele locaties waar mensen in groten getale bijeenkomen (bijv. openbare ruimten, ziekenhuizen, scholen, sportstadions, culturele centra, cafés en restaurants, winkelcentra en vervoersknooppunten). Deze locaties zijn, gezien hun aard, kwetsbaar en kunnen moeilijk worden beschermd; kenmerkend is ook dat de kans groot is dat er bij een aanslag massaal veel slachtoffers vallen. Om al die redenen hebben de terroristen een voorkeur voor deze doelwitten. De dreiging van toekomstige aanslagen tegen zachte doelwitten, waaronder het vervoer, blijft hoog. Dit wordt bevestigd door de beschikbare beoordelingen, onder meer het rapport van Europol over wijzigingen in de werkwijze van IS[4].

In de Europese veiligheidsagenda van 2015 en de mededeling van 2016 over de Veiligheidsunie is benadrukt dat er, voor de bescherming van zachte doelwitten, meer moet worden ingezet op een betere beveiliging en op het gebruik van innovatieve detectieapparatuur en -technologie. De Commissie heeft ernaar gestreefd de lidstaten te helpen bij de ontwikkeling van betere instrumenten om aanvallen tegen zachte doelwitten te voorkomen en daarop te reageren, en heeft de lidstaten aangemoedigd om de beste praktijken onderling uit te wisselen. Deze activiteiten hebben inmiddels geresulteerd in operationele handboeken en richtsnoeren. Op dit ogenblik is de Commissie, in nauwe samenwerking met deskundigen van de lidstaten, bezig met het opstellen van een uitgebreide handleiding over veiligheidsprocedures en van templates voor de verschillende zachte doelwitten (bijv. grote winkelcentra, ziekenhuizen, sport- en cultuurevenementen). Doel hiervan is de lidstaten begin 2017 richtsnoeren voor de bescherming van zachte doelwitten te geven, op basis van de beste praktijken in de lidstaten.

Parallel daarmee organiseert de Commissie in februari de eerste workshop over de bescherming van zachte doelwitten waaraan de nationale autoriteiten zullen deelnemen. Het is de bedoeling om tijdens deze workshop informatie uit te wisselen en beste praktijken uit te werken met betrekking tot de complexe kwestie van de bescherming van zachte doelwitten en de openbare veiligheid en beveiliging. Voorts financiert de Commissie uit het Fonds voor interne veiligheid een proefproject van België, Nederland en Luxemburg in verband met de oprichting van een regionaal excellentiecentrum voor gespecialiseerde rechtshandhavingsinterventies. Dit centrum zal opleiding bieden aan politieagenten, die vaak de eerste hulpverleners zijn bij een aanval.

Een essentieel onderdeel van de werkzaamheden van de Commissie op het gebied van de civiele bescherming betreft de wijze waarop moet worden gereageerd op aanslagen tegen zachte doelwitten. In december heeft de Commissie aangekondigd welke acties zij samen met de lidstaten wil ondernemen om in de onmiddellijke nasleep van terroristische aanslagen de EU-burgers te beschermen en de crisisgevoeligheid te verminderen. Deze acties zullen leiden tot een sterkere coördinatie tussen alle actoren die bij het beheer van de gevolgen van aanslagen betrokken zijn, en de Commissie heeft beloofd de inspanningen van de lidstaten te ondersteunen door het faciliteren van gezamenlijke

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, november 2016 – Publieksinformatie van Europol, te vinden op: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

opleidingen en oefeningen en door te zorgen voor een voortdurende dialoog via de bestaande contactpunten en deskundigengroepen. De Commissie zal ook, in het kader van het Uniemechanisme voor civiele bescherming, steun verlenen voor de ontwikkeling van gespecialiseerde modules om op terroristische aanvallen te reageren. Tevens zal zij initiatieven steunen om de geleerde lessen te delen en het publiek bewust te maken.

Samen met de lidstaten zal de Commissie ook nagaan welke EU-steun kan worden aangewend om rond mogelijke zachte doelwitten weerbaarheid te helpen opbouwen en veiligheid te versterken. De lidstaten zouden ook, in overeenstemming met het beleid van de EU en de EIB-groep, kunnen vragen om financiering door de Europese Investeringsbank (EIB) (met inbegrip van het Europees Fonds voor strategische investeringen). Voor elk project zouden de normale besluitvormingsprocedures gelden die in de wetgeving zijn vastgelegd.

Met betrekking tot de specifieke zachte doelwitten in verband met publieke vervoersruimten, zoals de openbaar toegankelijke delen van luchthavens of treinstations, is tijdens de speciale workshop van de Commissie in november 2016, waaraan zeer uiteenlopende belanghebbenden hebben deelgenomen, benadrukt dat het noodzakelijk is een evenwicht te bewaren tussen de veiligheidsbehoeften, het reizigersgemak en de uitbating van de vervoersdiensten. In de conclusies wordt gewezen op het belang van de totstandbrenging van een veiligheidscultuur, waarbij niet alleen het personeel, maar ook de passagiers betrokken zijn, op het belang van lokale risicobeoordelingen als basis voor de vaststelling van passende tegenmaatregelen en op de noodzaak om de communicatie tussen alle betrokken partijen te verbeteren.

IV. OMGAAN MET CYBERDREIGINGEN

Cybercriminaliteit en cyberaanvallen zijn belangrijke uitdagingen voor de Unie. Actie daartegen op EU-niveau kan bijdragen tot het versterken van onze collectieve weerbaarheid. Elke dag hebben cyberbeveiligingsincidenten ernstige nadelige gevolgen voor het leven van burgers en brengen zij de Europese economie en bedrijven zware economische schade toe. Cyberaanvallen zijn een essentieel onderdeel van hybride bedreigingen; precies getimed in combinatie met fysieke bedreigingen (bijvoorbeeld in het kader van terrorisme) kunnen zij een verwoestend effect hebben. Zij kunnen ook een rol spelen in het destabiliseren van een land of het verzwakken van de politieke instellingen en de fundamentele democratische processen van dat land. Naarmate wij meer gebruikmaken van onlinetechnologieën, zal onze kritieke infrastructuur (gaande van ziekenhuizen tot kerncentrales) steeds kwetsbaarder worden.

De EU-strategie voor cyberbeveiliging van 2013 is een van de fundamentele beleidsinstrumenten waarmee de EU reageert op de uitdagingen inzake cyberbeveiliging. Centraal staat de richtlijn betreffende de beveiliging van netwerk- en informatiesystemen (NIS)[5], die in juli vorig jaar is aangenomen. Die richtlijn legt de grondslag om op EU-niveau beter samen te werken en de cyberweerbaarheid te verhogen door het ondersteunen van samenwerking en uitwisseling van informatie tussen de lidstaten, het

[5] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

bevorderen van de operationele samenwerking bij specifieke cyberbeveiligingsincidenten en het delen van informatie over risico's. Om te zorgen voor een consistente uitvoering in de verschillende sectoren en over de grenzen heen organiseert de Commissie in februari de eerste vergadering van de NIS-samenwerkingsgroep met de lidstaten.

In april 2016 hebben de Commissie en de hoge vertegenwoordiger van de EU een gezamenlijk kader voor de bestrijding van hybride bedreigingen[6] goedgekeurd, met 22 voorgestelde operationele maatregelen die gericht zijn op bewustmaking, opbouw van weerbaarheid, een betere respons op crisissituaties en versterking van de samenwerking tussen de EU en de NAVO. Op vraag van de Raad zullen de Commissie en de hoge vertegenwoordiger van de EU uiterlijk in juli 2017 een voortgangsverslag voorleggen.

De Commissie stimuleert en ondersteunt ook technologische innovatie, onder meer door gebruik te maken van de onderzoeksfondsen van de EU, om aan te zetten tot het vinden van nieuwe oplossingen en het creëren van nieuwe technologieën die de weerbaarderheid tegen cyberaanvallen kunnen versterken (bijv. projecten waarbij beveiliging al tijdens de ontwerpfase wordt ingebouwd ("security by design"). Afgelopen zomer heeft zij met het bedrijfsleven een publiek-privaat partnerschap voor cyberbeveiliging aangegaan, waarmee 1,8 miljard EUR gemoeid is[7].

Wat vervoer betreft, is digitalisering een belangrijke aanjager voor de dringend noodzakelijke transformatie van het huidige vervoersysteem. Het snelle tempo van de digitalisering biedt tal van voordelen, maar maakt het vervoer ook kwetsbaarder voor risico's op het gebied van cyberbeveiliging of cyberveiligheid. Er worden vele acties ondernomen om de impact van de dreiging op verschillende niveaus te beperken, met name in de luchtvaart, maar ook voor het zeevervoer, de binnenscheepvaart, het spoorweg- en het wegvervoer[8]. Nu is het zaak de activiteiten van de verschillende belanghebbenden die bij het versterken van de uiteenlopende aspecten van de cyberweerbaarheid betrokken zijn, verder te verduidelijken, te harmoniseren en aan te vullen.

Meer in het algemeen, en gezien de snel veranderende aard van de dreiging, zullen de Commissie en de hoge vertegenwoordiger van de EU de komende maanden, voortbouwend op de EU-strategie voor cyberbeveiliging van 2013, bepalen welke maatregelen nodig zijn om te zorgen voor een doeltreffende EU-brede respons op deze bedreigingen.

---

6 JOIN (2016)18.

7 Aangekondigd in de mededeling "Versterken van het Europese cyberbeveiligingssysteem" van 2016, COM(2016) 410 final.

8 Voorbeelden hiervan zijn: internationale richtsnoeren, zoals die welke zijn opgesteld door de Internationale Maritieme Organisatie of via een onlangs aangenomen resolutie van de ICAO (gezamenlijke initiatieven van de EU en de VS), melding van incidenten, waarvoor het Europees Agentschap voor de veiligheid van de luchtvaart momenteel een proactievere modus ontwikkelt, en ingebouwde cyberbeveiliging ("cyber security by design"), die wordt toegepast bij de nieuwe systemen die worden ontwikkeld, zoals in het kader van het masterplan voor luchtverkeersbeheer van de gemeenschappelijke onderneming Sesar.

V. PERSOONSGEGEVENS BESCHERMEN EN TEGELIJK BIJDRAGEN AAN DE EFFICIËNTIE VAN STRAFRECHTELIJKE ONDERZOEKEN

De richtlijn inzake gegevensbescherming op politieel en strafrechtelijk gebied[9] is een bouwsteen voor de bestrijding van terrorisme en zware criminaliteit. Op basis van een in de richtlijn vastgestelde gemeenschappelijke norm voor gegevensbescherming zullen de rechtshandhavingsautoriteiten van de lidstaten relevante gegevens vlot kunnen uitwisselen, terwijl de gegevens van slachtoffers, getuigen en verdachten van misdrijven naar behoren worden beschermd.

Voorts heeft de Commissie, om zowel natuurlijke personen als bedrijven een hoge mate van vertrouwelijkheid van de communicatie te garanderen en om voor alle marktspelers een gelijk speelveld te creëren, zoals uiteengezet in de strategie voor de digitale eengemaakte markt van april 2015, op 11 januari 2017 de voorgestelde **e-privacyverordening**[10] aangenomen (ter vervanging van Richtlijn 2002/58/EG). Net zoals in de huidige richtlijn wordt in de herziene e-privacyverordening de algemene verordening gegevensbescherming[11] nader uitgewerkt en wordt een kader vastgesteld voor de bescherming van de persoonlijke levenssfeer en de persoonsgegevens in de sector van de elektronische communicatie.

Door deze herziening worden alle elektronische-communicatiegegevens, zelfs indien de communicatie secundair is, geacht vertrouwelijk of voor beperkte verspreiding te zijn, ongeacht of zij worden doorgestuurd via de traditionele telecommunicatiediensten of via andere zogeheten "over-the-top"-diensten (OTT-diensten), die functioneel gelijkwaardig zijn (zoals Skype en Whatsapp) en voor vele gebruikers vaak inwisselbaar zijn geworden met de diensten van de gewone telecomoperatoren[12]. Tot de verplichtingen die aan dienstenaanbieders worden opgelegd – naast eerbiediging van de privacykeuzen van hun klanten wat betreft gebruik, opslag en verwerking van hun gegevens – behoort ook de verplichting dat dienstenaanbieders die buiten de EU zijn gevestigd, een vertegenwoordiger in een lidstaat moeten aanwijzen. Hierdoor zullen de lidstaten het voor de rechtshandhavings- en justitiële autoriteiten ook gemakkelijker kunnen maken om met de dienstenaanbieders samen te werken voor het verkrijgen van toegang tot elektronisch bewijsmateriaal (zie hieronder).

---

9 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. De richtlijn, die van kracht is sinds 5 mei 2016, moet uiterlijk op 6 mei 2018 door de lidstaten zijn omgezet. De Commissie heeft met de lidstaten een deskundigengroep opgericht om over de omzetting van deze richtlijn van gedachten te wisselen.

10 Verordening met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, COM(2017) 10.

11 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), die van toepassing zal worden op 25 mei 2018.

12 Hierbij wordt de benadering gevolgd die is geformuleerd in het voorstel voor een richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie (COM(2016) 590 final), dat de Commissie op 14 september 2016 heeft ingediend (het telecommunicatiepakket).

Zoals in het kader van de huidige e-privacyregels zal de toegang van de rechtshandhavings- en justitiële autoriteiten tot belangrijke elektronische informatie die nodig is om misdrijven te onderzoeken, worden geregeld door de uitzondering waarin artikel 11 van de voorgestelde e-privacyverordening voorziet[13]. Deze bepaling maakt het mogelijk om via EU-recht of nationaal recht de vertrouwelijkheid van de communicatie te beperken indien een dergelijke beperking een noodzakelijke en evenredige maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te beschermen, strafbare feiten te voorkomen, op te sporen, te onderzoeken of te vervolgen, of strafrechtelijke sancties uit te voeren. Na de nietigverklaring, in 2014, van de richtlijn inzake gegevensbewaring[14] door het Europees Hof van Justitie (EHvJ) is deze bepaling van bijzonder belang voor de nationale voorschriften inzake **gegevensbewaring**, d.i. om aanbieders van telecommunicatiediensten te verplichten communicatiegegevens gedurende een bepaalde periode bij te houden met het oog op het verlenen van toegang voor rechtshandhavingsdoeleinden. Sinds het arrest van het EHvJ bestond er geen EU-instrument voor gegevensbewaring meer; sommige lidstaten hebben dan hun eigen nationale wetgeving inzake gegevensbewaring vastgesteld. De Zweedse en de Britse wetgeving inzake gegevensbewaring werden aangevochten voor het EHvJ, dat op 21 december zijn arrest in de zaak *Tele*2 heeft uitgebracht[15]. Volgens het EHvJ is nationale wetgeving die, om criminaliteit te bestrijden, voorziet in algemene en ongedifferentieerde bewaring van alle verkeers- en locatiegegevens van de abonnees en gebruikers met betrekking tot alle elektronische communicatiemiddelen, onverenigbaar met het EU-recht. De gevolgen van de uitspraak worden nu onderzocht en de Commissie zal richtsnoeren verstrekken over de wijze waarop nationale wetgeving inzake gegevensbewaring kan worden opgesteld die in overeenstemming is met de uitspraak van het Hof.

Criminaliteit laat digitale sporen achter die kunnen dienen als bewijs in gerechtelijke procedures; de elektronische communicatie tussen verdachten vormt voor rechtshandhavingsautoriteiten en openbare aanklagers vaak het enige aanknopingspunt. Het verkrijgen van toegang tot **elektronisch bewijsmateriaal** kan evenwel, vooral als die gegevens in het buitenland of in een cloud worden opgeslagen, technisch en juridisch ingewikkeld en procedureel gezien vaak omslachtig zijn, wat een obstakel is voor speurders, die snel moeten kunnen optreden. Om deze problemen aan te pakken onderzoekt de Commissie momenteel oplossingen die speurders in staat stellen grensoverschrijdende elektronische gegevens te verkrijgen. Mogelijke oplossingen zijn het doeltreffender maken van wederzijdse rechtshulp, het vinden van manieren om rechtstreeks samen te werken met aanbieders van internetdiensten en het voorstellen van criteria voor de vaststelling en handhaving van de jurisdictie in de cyberruimte, met volledige inachtneming van de toepasselijke voorschriften inzake

[13] Artikel 11, lid 1, de "clausule inzake gegevensbewaring", is ongewijzigd overgenomen van artikel 15 van de e-privacyrichtlijn en op één lijn gebracht met de eisen van de algemene verordening gegevensbescherming. Een dergelijke beperking moet rekening houden met de wezenlijke inhoud van de grondrechten en noodzakelijk, passend en evenredig zijn.

[14] Arrest van het EHvJ van 8 april 2014 in de gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland*.

[15] Arrest van het EHvJ van 21 december 2016 in de gevoegde zaken C-203/15 en C-698/15, *Tele*2.

gegevensbescherming.[16] Op 9 december 2016 heeft de Commissie bij de Raad Justitie en Binnenlandse Zaken verslag uitgebracht over de geboekte vooruitgang[17].

Uitgebreid (nog lopend) overleg met deskundigen heeft het de Commissie mogelijk gemaakt om de verschillende, vaak complexe problemen in verband met de toegang tot elektronisch bewijsmateriaal in kaart te brengen, een beter inzicht in de huidige regels en praktijken in de lidstaten te krijgen en te bepalen wat de mogelijke beleidsopties zijn. Het voortgangsverslag geeft een overzicht van de ideeën die tot dusver bij het verzamelen van informatie en tijdens het deskundigenoverleg naar voren zijn gekomen, en die de Commissie, in overleg met de belanghebbenden, in de komende maanden verder zal onderzoeken. Zoals aangekondigd in haar werkprogramma zal de Commissie in 2017 een initiatief voorleggen.

VI. CONCLUSIE

Het volgende verslag, dat uiterlijk op 1 maart moet zijn voorgelegd, biedt de kans om na te gaan welke vorderingen zijn gemaakt bij de uitwerking van deze en andere belangrijke werkgebieden.

[16] Zoals toegezegd in de Europese veiligheidsagenda (COM(2015) 185 final) en in de mededeling van de Commissie "Uitvoering van de Europese veiligheidsagenda ter bestrijding van terrorisme en ter voorbereiding van een echte en doeltreffende Veiligheidsunie" (COM(2016) 230 final).

[17] In zijn conclusies over de verbetering van de strafrechtpleging in de cyberruimte van 9 juni 2016 heeft de Raad er bij de Commissie op aangedrongen om concrete stappen te ondernemen, een gemeenschappelijke Europese aanpak uit te stippelen en uiterlijk in juni 2017 resultaten voor te leggen.