EUROPA-
KOMMISSIONEN

Bruxelles, den 25.1.2017
COM(2017) 41 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, DET EUROPÆISKE RÅD OG RÅDET

Fjerde statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion

Fjerde statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion

I. INDLEDNING

Dette er den fjerde månedlige statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion, og den beskriver udviklingen i to hovedsøjler: *bekæmpelse af terrorisme og organiseret kriminalitet og de midler, der støtter dem og styrkelse af vores forsvar og opbygning af modstandsdygtighed over for disse trusler*. Denne rapport fokuserer på fire nøgleområder: informationssystemer og interoperabilitet, beskyttelse af bløde mål, cybertrusler og databeskyttelse i forbindelse med kriminalefterforskning.

Angrebet i december på Berlins julemarked har atter fremhævet alvorlige svagheder i vores informationssystemer, der kræver omgående indgriben primært på EU-plan for at hjælpe de nationale grænsemyndigheder og retshåndhævende myndigheder på stedet med mere effektivt at udføre deres krævende job. Det er nødvendigt omgående at afhjælpe de praktiske implementeringssvagheder, at de forskellige informationssystemer ikke er indbyrdes forbundne — hvilket giver angribere mulighed for at bruge flere identiteter for at bevæge sig ubemærket rundt, herunder når de krydser grænser — og at oplysningerne rutinemæssigt ikke uploades af medlemsstaterne til de relevante EU-databaser. Det er desuden også nødvendigt at arbejde videre på retshåndhævende foranstaltninger vedrørende grænserne og tilbagesendelse af personer, der har fået afslag på deres asylansøgning[1].

For så vidt angår beskyttelse af bløde mål, vil Kommissionen fremskynde arbejdet med at samle eksperter fra medlemsstaterne til at udveksle bedste praksis og fastsætte standardretningslinjer.

De cybertrusler, som EU står over for, bliver bredt dækket i medierne, og denne rapport ser på de forskellige indsatsområder, der allerede arbejdes på. Dette omfatter både forebyggelsessiden — gennem samarbejde med erhvervslivet for at fremme sikkerheden ved udformning og gennemførelse af direktivet om net- og informationssikkerhed — og ved at fremme samarbejde mellem medlemsstaterne og internationale organisationer og partnere om håndteringen af cyberangreb, når disse finder sted. Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik vil i de kommende måneder på basis af EU's cybersikkerhedsstrategi fra 2013 finde frem til, hvilke foranstaltninger der er nødvendige for at skabe en effektiv EU-ordning for at imødegå disse trusler.

Beskyttelse af enkeltpersoners privatliv og personoplysninger er en grundlæggende rettighed og dermed en hjørnesten i ethvert skridt hen imod en ægte sikkerhedsunion. Databeskyttelsesdirektivet for politimyndigheder og det strafferetlige område, der blev vedtaget i april 2016, sikrer en fælles høj standard for databeskyttelse og vil derfor lette gnidningsløs udveksling af relevante oplysninger mellem medlemsstaternes retshåndhævende myndigheder. Kommissionen har også indledt en revision af e-datadirektivet som led i sin datapakke for at få direktivets bestemmelser til at omfatte alle udbydere af elektronisk kommunikation og bringe dets bestemmelser i overensstemmelse

[1] Kommissionen vil i de kommende uger fremskynde fremlæggelsen af en revideret handlingsplan for tilbagesendelser, jf. rapporten fra Kommissionen til Europa-Parlamentet, Det Europæiske Råd og Rådet om driften af den europæiske grænse- og kystvagt, COM(2017) 42.

med den generelle forordning om databeskyttelse. Forslaget er udformet, så det sikrer privatlivets fred i forbindelse med elektronisk kommunikation, samtidig med at forslaget fremlægger de grunde, der kan lede til begrænsninger i e-dataforordningens anvendelsesområde, herunder hensynet til national sikkerhed eller kriminalefterforskninger.

II. STYRKELSE AF INFORMATIONSSYSTEMER OG INTEROPERABILITET

I kommissionsformand Jean-Claude Junckers tale om Unionens tilstand i september 2016 og konklusionerne fra Det Europæiske Råds møde i december 2016 nævnes vigtigheden af at afhjælpe de nuværende mangler i informationsstyringen og af at forbedre de **eksisterende informationssystemers interoperabilitet og indbyrdes forbundethed**. Det presserende behov for at forbinde EU's eksisterende databaser er endnu en gang blevet tydeliggjort af de nylige begivenheder, ikke mindst så man kan give grænse- og retshåndhævelsesmyndigheder på stedet de redskaber, som de har brug for til at opdage identitetsmisbrug. For eksempel anvendte gerningsmanden bag terrorangrebet i Berlin i december 2016 mindst 14 forskellige identiteter og kunne bevæge sig mellem medlemsstaterne uden at blive opdaget. Der er et klart behov for, at EU's nuværende og fremtidige informationssystemer skal være søgbare, samtidig med at man anvender biometriske identifikatorer, så terrorister og forbrydere ikke længere kan benytte forskellige identiteter.

Kommissionen har i denne henseende i april 2016 indledt arbejdet med sine forslag om "stærkere og mere intelligente informationssystemer for grænser og sikkerhed"[2]. Derved konstateredes der mangler med hensyn til funktionaliteterne i de eksisterende systemer, huller i EU's datastyringsstruktur, problemer med et komplekst landskab af forskelligt styrede informationssystemer og en overordnet opsplitning, som følge af at de eksisterende systemer i sin tid blev udformet hver for sig frem for som et samlet hele. Som en del af denne proces nedsatte Kommissionen **Ekspertgruppen på Højt Niveau vedrørende Informationssystemer og Interoperabilitet** med deltagelse af EU-agenturer, medlemsstater og relevante interessenter. Den 21. december 2016[3] redegjorde formanden i en foreløbig rapport for gruppens **foreløbige resultater**, der omfatter den prioriterede mulighed, at man opretter en fælles søgeportal, hvor nationale retshåndhævende myndigheder og grænsemyndigheder kan foretage samtidige søgninger i de eksisterende EU-databaser og informationssystemer. Den foreløbige rapport sætter også fokus på vigtigheden af datakvalitet — eftersom informationssystemerne kun er så effektive som kvaliteten og formatet af de data, der indberettes — og indeholder anbefalinger, der skal forbedre datakvaliteten i EU's systemer gennem automatiseret kontrol af datakvaliteten.

Kommissionen vil snarest følge op på muligheden af at oprette en fælles søgeportal og sammen med EU's agentur for den Operationelle Forvaltning af Store IT-Systemer, eu-LISA, begynde arbejdet på en portal, der kan foretage samtidige søgninger i alle de relevante eksisterende EU-systemer. En relateret undersøgelse skulle være klar senest i

[2] Meddelelsen "Stærkere og mere intelligente informationssystemer for grænser og sikkerhed", COM(2016) 205 Final.

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

juni. Den kan være basis for at udforme og afprøve en prototype af portalen inden årets udgang. Kommissionen mener, at Europol parallelt hermed bør fortsætte sit arbejde med en grænseflade, der kan gøre medlemsstaternes medarbejdere ved grænserne i stand til automatisk at søge i Europols databaser, samtidigt med at de søger i deres egne nationale systemer.

Arbejdet på at gøre informationssystemerne interoperationelle sigter mod at afhjælpe den nuværende fragmentering i EU's struktur for forvaltning af data til grænsekontrol og -sikkerhed og de dermed forbundne blinde vinkler. Når databaser benytter en fælles database med personoplysninger — som det er planen at gøre i det foreslåede ind- og udrejsesystem og det foreslåede EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS) — kan en person kun kan være registreret under én enkelt identitet i de forskellige databaser, hvilket forhindrer anvendelsen af forskellige falske identiteter. Kommissionen har — som et første skridt som foreslået i de foreløbige resultater fra Ekspertgruppen på Højt Niveau — anmodet eu-LISA om at analysere de tekniske og operationelle aspekter ved at indføre en delt biometrisk tjeneste. En sådan tjeneste vil muliggøre søgninger på tværs af forskellige databaser med biometriske data, hvilket kan afsløre, at den pågældende person har anvendt falske identiteter i et andet system. Derudover bør Ekspertgruppen på Højt Niveau nu vurdere, om det er nødvendigt, teknisk gennemførligt og rimeligt at udvide det **fælles identitetsregister**, der er planlagt for ind- og udrejsesystemet og ETIAS, til andre systemer. Et sådant fælles identitetsregister vil, udover biometriske data lagret i den biometriske tjeneste, også omfatte alfanumeriske identitetsoplysninger. Gruppen skal fremlægge sine konklusioner herom i sin endelige rapport inden udgangen af april 2017.

Nylige sikkerhedsmæssige begivenheder fremhæver behovet for at genoverveje spørgsmålet om **obligatorisk dataudveksling** mellem medlemsstaterne. Kommissionens forslag fra december 2016 om at styrke **Schengeninformationssystemet** indeholder for første gang en forpligtelse for medlemsstaterne til at udsende advarsler om personer, der er knyttet til terrorhandlinger. Det er vigtigt, at medlovgiverne nu arbejder hen imod en hurtig vedtagelse af de foreslåede foranstaltninger. Kommissionen er rede til at undersøge, om obligatorisk dataudveksling skal indføres for andre EU-databaser.

III. BESKYTTELSE AF BLØDE MÅL MOD TERRORANGREB

Angrebet i Berlin var det seneste i EU mod såkaldte bløde mål, der typisk er civile steder, hvor mennesker samles i store grupper (f.eks. offentlige rum, hospitaler, skoler, sportsstadioner, kulturcentre, caféer og restauranter, indkøbscentre og transportknudepunkter). Disse steder er på grund af deres art sårbare og vanskelige at beskytte, og de er også er kendetegnet ved stor sandsynlighed for et stort antal døde og sårede i tilfælde af et angreb. Disse grunde gør dem populære blandt terrorister. Truslen om fremtidige angreb på bløde mål, herunder transport, er fortsat stor, jf. de tilgængelige vurderinger, herunder Europols rapport om udviklingen i Daeshs modus operandi[4].

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, november 2016 – Europol Public Information, tilgængelig her: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited.

Den europæiske dagsorden om sikkerhed fra 2015 og Kommissionens meddelelse fra 2016 om sikkerhedsunionen fremhæver behovet for at forbedre sikkerheden og anvende innovative detektionsværktøjer og -teknologier til at beskytte bløde mål. Kommissionen har gjort en indsats for at støtte og tilskynde til udveksling af bedste praksis medlemsstaterne imellem om udvikling af bedre redskaber til at forebygge og reagere på angreb mod bløde mål. Som led i dette arbejde er der blevet udarbejdet vejledninger og håndbøger med retningslinjer. Kommissionen udvikler nu i tæt samarbejde med medlemsstaternes eksperter en omfattende håndbog om sikkerhedsprocedurer og -modeller, der passer til forskellige bløde mål (f.eks. indkøbscentre, hospitaler, sportsbegivenheder og kulturelle arrangementer). Målet er at udstede vejledning til medlemsstaterne i begyndelsen af 2017 om beskyttelse af bløde mål baseret på medlemsstaternes bedste praksis.

Kommissionen vil parallelt hermed sammen med de nationale myndigheder afholde den første workshop i februar om beskyttelse af bløde mål med henblik på at udveksle oplysninger og udvikle god praksis for beskyttelse af bløde mål og offentlig sikkerhed, der er et komplekst emne. Kommissionen yder også støtte til et pilotprojekt, som Belgien, Nederlandene og Luxembourg gennemfører under Fonden for Intern Sikkerhed med henblik på at oprette et regionalt ekspertisecenter for særlige retshåndhævelsesaktioner, der kan uddanne politifolk, der ofte udgør det første responsled i tilfælde af angreb.

Beredskab ved angreb på bløde mål er et centralt element i Kommissionens civilbeskyttelsesarbejde. Kommissionen annoncerede i december de foranstaltninger, som den agter at træffe sammen med medlemsstaterne for at beskytte EU-borgere og mindske sårbarhed umiddelbart efter terrorangreb. Disse foranstaltninger vil styrke koordineringen mellem alle de aktører, der er involveret i håndteringen af følgerne af angreb, og Kommissionen har givet tilsagn om at støtte medlemsstaternes tiltag ved at fremme fælles uddannelse og øvelser og ved at sikre en vedvarende dialog via eksisterende kontaktpunkter og ekspertgrupper. Kommissionen vil også inden for rammerne af EU's civilbeskyttelsesordning støtte udviklingen af specialiserede uddannelsesmoduler om beredskab ved terrorangreb og initiativer til at udveksle erfaringer og øge offentlighedens bevidsthed.

Kommissionen vil også sammen med medlemsstaterne undersøge, hvilken EU-støtte der kan mobiliseres for at bidrage til at opbygge modstandsdygtigheden og styrke sikkerheden omkring potentielle bløde mål. Medlemsstaterne kan også ansøge om finansiering fra Den Europæiske Investeringsbank (EIB) (herunder Den Europæiske Fond for Strategiske Investeringer) i overensstemmelse med EU's og EIB-Gruppens politikker. Alle projekterne vil være underlagt de normale beslutningsprocedurer, som er fastsat i lovgivningen.

For så vidt angår de specifikke bløde mål i forbindelse med områder med offentlig transport, såsom offentlige dele af lufthavne eller jernbanestationer, gjorde Kommissionens særlige workshop i november 2016, hvori en bred vifte af interessenter deltog, opmærksom på behovet for at opretholde balancen mellem sikkerhedsbehov, passagerernes bekvemmelighed og transportdriften. Konklusionerne understreger betydningen af at opbygge en sikkerhedskultur, der omfatter ikke blot personale, men også passagerer, vigtigheden af lokale risikovurderinger som grundlag for at fastlægge passende modforanstaltninger og behovet for at forbedre kommunikationen mellem alle involverede parter.

IV. IMØDEGÅELSE AF CYBERTRUSLER

Cyberkriminalitet og cyberangreb er centrale udfordringer for Unionen, og taget under et er det et område, hvor en indsats på EU-plan kan være med til at styrke vores fælles modstandsdygtighed. Hver eneste dag forvolder cybersikkerhedshændelser alvorlig skade på borgeres liv og forårsager betydelig økonomisk skade for den europæiske økonomi og erhvervslivet. Cyberangreb er et centralt element i hybride trusler. Når de synkroniseres til at finde sted samtidig med fysiske trusler, f.eks. i forbindelse med terrorisme, kan de have en ødelæggende virkning. De kan også bidrage til at destabilisere et land eller udfordre dets politiske institutioner og grundlæggende demokratiske processer. Vores kritiske infrastruktur (lige fra hospitaler til atomkraftværker) vil blive stadig mere sårbar, i takt med at vi i stigende grad bliver afhængige af onlineteknologier.

EU's cybersikkerhedsstrategi fra 2013 udgør en del af de centrale politiske svar på cybersikkerhedsudfordringerne. Den centrale foranstaltning er direktivet om net- og informationssikkerhed (NIS)[5], der blev vedtaget i juli sidste år. Det udgør fundamentet for forbedret samarbejde på EU-plan og cybermodstandsdygtighed ved at støtte samarbejde og informationsudveksling mellem medlemsstaterne og ved at fremme operationelt samarbejde i forbindelse med specifikke cybersikkerhedshændelser og informationsudveksling omkring risici. Kommissionen vil for at sikre konsekvent gennemførelse på tværs af forskellige sektorer og på tværs af grænser holde det første møde i NIS-samarbejdsgruppen med medlemsstaterne i februar.

Kommissionen og Unionens højtstående repræsentant vedtog i april 2016 en fælles ramme for imødegåelse af hybride trusler[6], der indeholdt forslag om 22 operationelle tiltag, der skal øge opmærksomheden, opbygge modstandsdygtigheden, forbedre reaktionerne i tilfælde af kriser og øge samarbejdet mellem EU og NATO. Kommissionen og Unionens højtstående repræsentant vil — som Rådet har anmodet om — fremlægge en rapport inden juli 2017 for at vurdere de gjorte fremskridt.

Kommissionen fremmer og støtter desuden teknologisk innovation, herunder ved at gøre brug af EU's forskningsmidler til at fremme nye løsninger og til at skabe nye teknologier, der kan bidrage til at styrke vores modstandsdygtighed over for cyberangreb (f.eks. projekter om design af sikkerhedssystemer). Vi lancerede sidste sommer et offentlig-privat partnerskab med industrien til 1,8 mia. EUR om cybersikkerhed[7].

Digitalisering inden for transportsektoren er ved at blive en vigtig drivkraft bag en påtrængt transformation af vore dages transportsystem. Den hastige digitalisering medfører mange fordele, men gør også transportsektoren mere sårbar over for cybersikkerhedsrisici. Talrige foranstaltninger er truffet for at mindske truslen på forskellige niveauer, særligt inden for luftfart, men også inden for transport til havs, på floder samt jernbane- og vejtransport[8]. Den sidste udfordring er yderligere at tydeliggøre,

---

5 Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

6 JOIN(2016) 18.

7 Dette initiativ blev annonceret i meddelelsen fra 2016 om modstandsdygtighed over for cyberangreb, COM(2016) 410 final.

8 Eksempler herpå er internationale retningslinjer, såsom dem, der er udviklet af Den Internationale Søfartsorganisation eller ved hjælp af en nyligt vedtaget ICAO-resolution efter et fælles initiativ fra EU og USA; rapportering om hændelser, som Det Europæiske Luftfartssikkerhedsagentur netop nu

ensrette og supplere den indsats, der gøres af de forskellige interessenter, der er engageret i at forbedre forskellige aspekter af modstandsdygtighed over for cyberangreb.

Kommissionens og Unionens højtstående repræsentant vil mere generelt — og i betragtning af truslernes hastigt skiftende karakter og på grundlag af EU's cybersikkerhedsstrategi fra 2013 — udpege de nødvendige tiltag, der kan skabe en effektiv reaktion i hele EU på disse trusler.

V. BESKYTTELSE AF PERSONOPLYSNINGER PARALLELT MED STØTTE TIL EFFEKTIV KRIMINALEFTERFORSKNING

Databeskyttelsesdirektivet for politimyndigheder og på det strafferetlige område[9] er en byggesten i kampen mod terrorisme og grov kriminalitet. Medlemsstaternes retshåndhævende myndigheder vil på baggrund af en fælles standard for databeskyttelse fastsat i direktivet let kunne udveksle relevante data, samtidig med at personoplysninger om ofre, vidner og mistænkte bliver beskyttet på passende vis.

Kommissionen har desuden den 11. januar vedtaget den foreslåede **e-dataforordning** (der erstatter direktiv 2002/58/EF)[10] for at sikre et højt niveau af fortrolighed for både enkeltpersoners og virksomheders kommunikation og ens spilleregler for alle markedsaktører, jf. strategien for det digitale indre marked fra april 2015. Den reviderede e-dataforordning præciserer — som det nuværende direktiv — den generelle forordning om databeskyttelse[11] og fastlægger en ramme for beskyttelse af privatlivets fred og personoplysninger i den elektroniske kommunikationssektor.

Efter denne revision vil alle elektroniske kommunikationsdata — også i tilfælde, hvor kommunikationen ikke er hovedformålet med aktiviteten — blive betragtet som fortrolige/begrænsede, om kommunikationen foregår gennem traditionelle telekommunikationstjenester eller gennem andre såkaldte over-the-top tjenester (OTT), der er funktionelt ækvivalente (f.eks. Skype og WhatsApp), der for mange brugere er blevet indbyrdes udskiftelige med normale teleoperatører[12]. De forpligtelser, som tjenesteudbyderne er underlagt, omfatter for tjenesteudbydere etableret uden for EU også

---

udvikler en mere reaktiv model for, samt design af cybersikkerhedssystemer for nye systemer, der er under udvikling, såsom SESAR-fællesforetagendets europæiske masterplan for lufttrafikstyring.

9 Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA. Direktivet, der har været i kraft siden den 5. maj 2016, skal være gennemført af medlemsstaterne senest den 6. maj 2018. Kommissionen har nedsat en ekspertgruppe med medlemsstaterne for at udveksle synspunkter om gennemførelsen af politidirektivet.

10 Forordning om privatlivets fred og elektronisk kommunikation, COM(2017) 10.

11 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), der anvendes fra den 25. maj 2018.

12 Det følger tilgangen i det foreslåede direktiv om oprettelse af en europæisk kodeks for elektronisk kommunikation, som Kommissionen fremlagde den 14. september 2016 (telekommunikationspakken), COM(2016) 590 final.

en forpligtelse til at udpege en repræsentant i en medlemsstat ud over forpligtelsen til at respektere klienternes valg vedrørende privatlivets fred for så vidt angår anvendelse, lagring og behandling af deres data. Det vil også give medlemsstaterne mulighed for at lette retshåndhævendes og retslige myndigheders samarbejde med tjenesteudbydere om adgang til elektroniske beviser (se nedenfor).

Retshåndhævendes og retslige myndigheders adgang til relevante elektroniske oplysninger, der er nødvendige for at efterforske kriminalitet, vil — som under de nuværende e-dataregler — være underlagt undtagelsen i artikel 11 i den foreslåede e-dataforordning[13]. Denne bestemmelse giver mulighed for gennem EU-lovgivning eller i national lovgivning at begrænse fortroligheden af kommunikation, når det er nødvendigt og rimeligt for at beskytte national sikkerhed, forsvar, offentlig sikkerhed og forebyggelse, efterforskning, afsløring eller retsforfølgning af straffelovsovertrædelser eller fuldbyrdelse af strafferetlige sanktioner. Bestemmelsen er navnlig relevant for de nationale regler for **datalagring**, dvs. for at forpligte udbydere af telekommunikationstjenester til at opbevare kommunikationsdata i en fastsat periode, så retshåndhævende myndigheder kan få adgang til dem, efter EU-Domstolens annullation af datalagringsdirektivet i 2014[14]. Der har siden da ikke været noget EU-instrument vedrørende datalagring, og nogle medlemsstater har vedtaget deres egen nationale datalagringslovgivning. De svenske og britiske datalagringslove blev anfægtet ved Domstolen, der afsagde dom om *Tele2* den 21. december[15]. Domstolen fandt, at national lovgivning, der af hensyn til kriminalitetsbekæmpelse tillader generel og vilkårlig lagring af alle abonnenters og brugeres trafikdata og lokaliseringsdata fra enhver form for elektronisk kommunikation, var i strid med EU-retten. Konsekvenserne af dommen er ved at blive analyseret, og Kommissionen vil udarbejde en vejledning i, hvordan nationale datalagringslove kan udarbejdes i overensstemmelse med dommen.

Kriminalitet efterlader sig digitale spor, der kan tjene som bevis i retssager. Elektronisk kommunikation mellem mistænkte er ofte det eneste spor, som retshåndhævende myndigheder og anklagere kan indsamle. Det kan dog ofte være både teknisk og juridisk komplekst og ofte proceduremæssigt besværligt at få adgang til **elektroniske beviser**, navnlig hvis de er lagret i udlandet eller i en sky, hvilket hindrer efterforskernes behov for at handle hurtigt. Til at håndtere disse udfordringer er Kommissionen for tiden i færd med at vurdere løsninger, der kan gøre efterforskere i stand til at indhente elektroniske beviser på tværs af grænser, herunder gøre den gensidige retshjælp mere effektiv, finde metoder til direkte samarbejde med internetudbydere og foreslå kriterier for at fastlægge og håndhæve kompetence i cyberspace i fuld overensstemmelse med gældende

[13] Se artikel 11, stk. 1 ("datalagringsbestemmelsen"), der er uændret i forhold til artikel 15 i e-datadirektivet og tilpasset kravene i den generelle forordning om databeskyttelse. Sådanne begrænsninger skal respektere kernen i de grundlæggende rettigheder og være nødvendige, hensigtsmæssige og forholdsmæssige.

[14] Domstolens dom i forenede sager C-293/12 og C-594/12 *Digital Rights Ireland* af 8. april 2014.

[15] Domstolens dom i forenede sager C-203/15 og C-698/15 *Tele2* af 21. december 2016.

databeskyttelsesregler[16]. Kommissionen aflagde den 9. december 2016 en fremskridtsrapport til Rådet for Retlige og Indre Anliggender[17].

En omfattende (og stadig igangværende) eksperthøringsproces har gjort det muligt for Kommissionen at kortlægge de forskellige og ofte komplekse problemer i forbindelse med adgang til elektroniske beviser, opnå en bedre forståelse af de nuværende regler og nuværende praksis i medlemsstaterne samt indkredse mulige politiske valgmuligheder. Statusrapporten indeholder en sammenfatning af de ideer, der er fremkommet indtil nu i forbindelse med informationsindsamlingen og eksperthøringen. Kommissionen vil sammen med interessenterne kigge nærmere på disse ideer over de kommende måneder. Kommissionen vil — som bebudet i Kommissionens arbejdsprogram — fremlægge et initiativ i 2017.

VI. KONKLUSION

Den næste rapport, der skal forelægges den 1. marts, vil give mulighed for at gøre status over gennemførelsen af disse og andre vigtige indsatsområder.

[16] Kommissionen har forpligtet sig hertil i den europæiske dagsorden om sikkerhed, COM(2015) 185 final, og i Kommissionens meddelelse om den europæiske dagsorden om sikkerhed for at bekæmpe terrorisme og bane vejen for en effektiv og ægte sikkerhedsunion, COM(2016) 230 final.

[17] Rådet har i sine konklusioner om styrkelse af strafferetten i cyberspace af 9. juni 2016 opfordret Kommissionen til at træffe konkrete foranstaltninger, udvikle en fælles EU-tilgang og fremlægge resultaterne i juni 2017.