JUSTITSMINISTERIET

Dato: 30. november 2020
Kontor: Internationalt kontor
Sagsbeh: Victor Granslev Christoffersen
Sagsnr.: 2020-3051-0052
Dok.: 1727731

Samlenotet vedrørende de sager inden for Justitsministeriets ansvarsområde, der forventes behandlet på rådsmødet (retlige og indre anliggender) den 14. december 2020

Side:

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Dagsordenspunkt 1: Forslag til Europa-Parlamentets og Rådets forordning om forebyggelse af udbredelsen af terrorrelateret indhold på nettet

Revideret notat. Ændringerne er markeret med streg i marginen.

Sagen er ikke omfattet af retsforbeholdet.

KOM (2018) 640

1. Resumé

På rådsmødet (retlige og indre anliggender) den 14. december 2020 forventes formandskabet at orientere om status for trilogforhandlingerne om forslaget og om eventuelle foreløbige aftaler, der på tidspunktet for rådsmødet måtte være indgået med Europa-Parlamentet. Forslaget er en del af en samlet sikkerhedspakke bestående af tre initiativer, der skal styrke de redskaber, som EU giver de nationale retshåndhævende myndigheder for at bekæmpe terrorisme og grænseoverskridende kriminalitet. Forslaget har til formål at skabe en klar og harmoniseret retlig ramme til at forebygge misbrug af hostingtjenester, herunder online-platforme, hvor udbredelse af terrorrelateret indhold på nettet finder sted, med henblik på at garantere et velfungerende digitalt indre marked. Sagen er ikke omfattet af retsforbeholdet. Det vurderes, at en vedtagelse af forslaget vil have visse økonomiske konsekvenser for Danmark. Det vurderes dog ikke umiddelbart, at forslaget vil have statsfinansielle konsekvenser af betydning. Forslaget vurderes at være i overensstemmelse med nærhedsprincippet. Fra dansk side er man overordnet set positiv over for forordningsforslaget. Det tillægges dog afgørende vægt, at problemet i forhold til det såkaldte uskrevne grundlovsforbud bliver løst forud for forordningens eventuelle vedtagelse. Fra dansk side arbejder man i kontekst af de aktuelle trilogforhandlinger for at finde en løsning, der sikrer, at Danmark vil kunne administrere ordningen i overensstemmelse med grundloven.

2. Baggrund

Kommissionens formand præsenterede i sin State of the Union-tale den 12. september 2018 en "sikkerhedspakke" bestående af tre initiativer til at styrke de redskaber, som EU giver de nationale retshåndhævende myndigheder for at bekæmpe terrorisme og grænseoverskridende kriminalitet. Kommissionens forslag til forordning om forebyggelse af udbredelsen af terrorrelateret online-indhold er et af initiativerne.

Forordningsforslaget er fremsat med hjemmel i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) artikel 114 om sikring af et velfungerende indre marked og er derfor ikke omfattet af Danmarks forbehold vedrørende retlige og indre anliggender. Forslaget skal behandles efter den almindelige lovgivningsprocedure i TEUF artikel 294, dvs. med Europa-Parlamentet som medlovgiver.

Arbejdet med at bekæmpe udbredelsen af terrorrelateret indhold online er indtil nu sket ved hjælp af frivillige ordninger mellem Kommissionen, medlemsstaterne og en række hostingtjenesteydere, herunder bl.a. Facebook, Google, Twitter og Microsoft, særligt i regi af EU's internetforum. EU's internetforum blev etableret af Kommissionen i december 2015 og har til formål at fremme medlemsstaternes og hostingtjenesteydernes frivillige samarbejde og tiltag for effektivt at reducere terrorrelateret onlineindhold og styrke civilsamfundets aktører med henblik på at øge mængden af effektive, alternative budskaber på nettet.

Kommissionen vedtog den 1. marts 2018 en henstilling om effektiv bekæmpelse af ulovligt indhold på internettet[1], som bygger videre på Kommissionens meddelelse om bekæmpelse af ulovligt indhold på nettet fra september 2017[2]. Baggrunden for henstillingen var, at der ifølge Kommissionen er behov for en øget indsats fra EU's side på området. Henstillingen indeholder konkrete anbefalinger til, hvordan udbydere af onlineplatforme og medlemsstater kan intensivere arbejdet med bekæmpelse af ulovligt indhold på nettet, herunder særligt terrorrelateret indhold. Kommissionen tilkendegav i forbindelse med vedtagelsen af henstillingen, at man ville overveje behovet for lovgivning på området.

Den 19. juni 2018 fremlagde Frankrig og Tyskland en erklæring om fremtidige tiltag i EU, hvor de to lande bl.a. opfordrede til indførelsen af lovgivning på EU-niveau for at bekæmpe terrorrelateret indhold på nettet. Erklæringen førte til, at medlemsstaternes stats- og regeringschefer på foranledning af Frankrig i DER-konklusioner af 28. juni 2018 bød Kommissionens planer om et lovgivningsforslag om fjernelse af indhold, som tilskynder til had og til at begå terrorhandlinger, velkommen.

[1] Henstilling af 1. marts 2018 om foranstaltninger til effektiv bekæmpelse af ulovligt indhold på nettet (KOM (2018)1177 endelig).
[2] Meddelelse af 28. september 2017 om bekæmpelse af ulovligt indhold på nettet (KOM (2017) 555 endelig).

Dertil opfordrede Det Europæiske Råd allerede i juni 2017 industrien til at udvikle nye teknologier og værktøjer til at forbedre den automatiske påvisning og fjernelse af indhold, som tilskynder til terroristiske aktiviteter. Derudover har Europa-Parlamentet i sin beslutning om onlineplatforme og det digitale indre marked af 15. juni 2017 opfordret de pågældende platforme "til at styrke foranstaltninger til bekæmpelse af ulovligt og skadeligt indhold" og opfordret Kommissionen til at fremlægge forslag til løsning af disse problemer.

Forordningsforslaget supplerer de eksisterende frivillige ordninger i regi af EU's internetforum og bygger videre på Kommissionens henstilling om bekæmpelse af ulovligt indhold på nettet fra marts 2018. Derudover supplerer forordningen de eksisterende regler på EU-niveau om bekæmpelse af ulovligt indhold på nettet.

Forhandlingerne om forordningsforslaget blev indledt den 25. september 2018 på arbejdsgruppeniveau i Rådet.

Forslaget er oversendt til Rådet i dansk sprogversion den 1. oktober 2018.

Forslagets bestemmelser om jurisdiktion til at udstede påbud og indberetninger rejser spørgsmål i forhold til grundloven, da forslaget indebærer, at en kompetent myndighed i en anden medlemsstat kan træffe en retligt bindende afgørelse i form af f.eks. et påbud om fjernelse af terrorrelateret indhold over for en hostingtjenesteyder i Danmark. Afgørelsen bliver bindende for hostingtjenesteyderen umiddelbart og uden, at en dansk myndighed bliver involveret først, hvilket ikke er muligt efter grundloven. Det skyldes, at danske myndigheder efter dansk statsret anses for enekompetente til at udøve myndighedsbeføjelser inden for det danske territorium (det såkaldte uskrevne grundlovsforbud). Sådanne beføjelser kan efter grundlovens § 20 overlades til mellemfolkelige myndigheder, f.eks. EU, men ikke til andre stater.

På rådsmødet (retlige og indre anliggender) den 6.-7. december 2018 vedtog Rådet sin generelle indstilling til forslaget.

På trods af den overordnede støtte til forslagets formål stemte Danmark imod Rådets generelle indstilling til forslaget på rådsmødet. Danmark fremsatte under rådsmødet en erklæring, der udtrykte støtte til forslagets formål og intention og præsenterede samtidig en model for et forslag til ændring af forordningsforslaget, som løser problemet i forhold til

grundloven, med henblik på, at ændringsforslaget indarbejdes i forbindelse med trilogforhandlingerne mellem Rådet, Kommissionen og Europa-Parlamentet. Forslaget i erklæringen indebærer en tilføjelse til forordningsforslagets bestemmelse om jurisdiktion, der tager højde for den særlige danske situation, ved at et påbud mv., inden det får virkning, sendes til en kompetent dansk myndighed, som herefter øjeblikkeligt videresender det til hostingtjenesteudbyderen i Danmark. Herved kan det sikres, at en dansk myndighed involveres, før et påbud mv. får virkning i Danmark.

Forhandlingerne med Europa-Parlamentet blev indledt i oktober 2019. Der har været en længere pause i forhandlingerne særligt grundet udbruddet af COVID-19. Bl.a. som følge af de seneste terrorangreb i Frankrig og Østrig i oktober og november 2020, er der igen kommet ny fremdrift i forhandlingerne. Det er derfor ikke usandsynligt, at der vil kunne opnås en politisk aftale inden udgangen af året.

Det er navnlig spørgsmålet om den grænseoverskridende virkning, der er i fokus i forhandlingerne mellem Rådet og Europa-Parlamentet. Herudover er ordningen med indberetninger også genstand for forhandlinger. For en nærmere beskrivelse af ordningen med indberetninger henvises til pkt. 3 nedenfor.

Fra dansk side arbejder man i kontekst af de aktuelle trilogforhandlinger for at finde en løsning, der sikrer, at Danmark vil kunne administrere ordningen i overensstemmelse med grundloven.

Der arbejdes således henimod, at Danmark i forbindelse med Rådets vedtagelse af forordningsforslaget vil afgive en erklæring om, hvordan forordningen vil blive administreret i Danmark.

Det bemærkes i den forbindelse, at det vurderes at kunne blive meget vanskeligt at få ændret selve forordningsteksten tilstrækkeligt til i sig selv at løse grundlovsproblematikken.

3. Formål og indhold

3.1. Forslaget generelt

Kommissionens oprindelige forordningsforslag har været genstand for en række drøftelser på arbejdsgruppeniveau. Den følgende gennemgang afspejler Rådets generelle indstilling til forordningsforslaget, der blev vedtaget på rådsmødet (retlige og indre anliggender) den 6.-7. december 2018. Det skal

i den forbindelse understreges, at forslaget aktuelt fortsat er under trilogforhandling, og at der løbende fremsættes kompromisforslag, der afviger fra Rådets generelle indstilling, og som beskrives nedenfor. Det er navnlig den grænseoverskridende virkning, der giver anledning til uenigheder i trilogforhandlingerne. Herudover er ordningen med indberetninger også genstand for divergerende holdninger.

Formålet med forordningsforslaget er at skabe en klar og harmoniseret retlig ramme til at forebygge misbrug af hostingtjenester til udbredelse af terrorrelateret indhold på internettet med henblik på at garantere et velfungerende digitalt indre marked.

Forordningsforslaget omfatter alle hostingtjenesteydere, som udbyder tjenester i EU, uanset om tjenesteyderen er etableret i eller uden for EU. Baggrunden for også at omfatte hostingtjenesteydere, der er etableret uden for Unionen, men som udbyder tjenester inden for Unionen, er, at en betydelig del af de hostingtjenesteydere, der eksponeres for terrorindhold på deres tjenester, er etableret i tredjelande.

3.2. Nærmere om forslagets centrale elementer

Terrorrelateret indhold

Begrebet "terrorrelateret indhold" er i forslaget defineret som materiale, der kan bidrage til at begå terrorhandlinger, som de er defineret i artikel 3, stk. 1, litra a-i, i direktiv (EU) 2017/541 om bekæmpelse af terrorisme, ved:

(1) Trussel om at begå terrorhandlinger
(2) opfordring til eller slåen til lyd for, som for eksempel forherligelse af terrorhandlinger, udførelse af terrorhandlinger, hvorved der forårsages fare for, at sådanne handlinger begås
(3) *hvervning af* personer eller en gruppe af personer til at begå eller bidrage til terrorhandlinger
(4) promovering af en terrorgruppes aktiviteter, navnlig ved at *hverve* personer eller en gruppe af personer til deltagelse i eller støtte til en terrorgruppes i den artikel 2, stk. 3, i direktiv (EU) 2017/541 fastsatte betydning kriminelle aktiviteter
(5) instruktioner i metoder eller teknikker til udførelse af terrorhandlinger

Udbredelse af terrorrelateret indhold er i forslaget defineret som tilrådighedsstillelse af terrorrelateret indhold til tredjepart via hostingtjenesteyderes tjenester.

Omfattede hostingtjenesteydere
Hostingtjenesteyder er i forslaget defineret som en udbyder af informationssamfundstjenester, som består i oplagring af information fra en tjenestemodtager på dennes anmodning og tilrådighedsstillelse af de lagrede informationer til tredjeparter, uanset om denne aktivitet udelukkende er af teknisk, automatisk eller passiv karakter. Sådanne udbydere af informationssamfundstjenester omfatter eksempelvis sociale medieplatforme, videostreamingtjenester, video-, billed- og lyddelingtjenester, fildeling og andre cloudtjenester, i det omfang de gør informationerne tilgængelige for tredjepart, og websteder, hvor brugerne kan kommentere og poste anmeldelser.

Forordningen gælder for alle hostingtjenesteydere, som udbyder tjenester i EU, uanset om tjenesteyderen er etableret i eller uden for EU.

Det afgørende for, at der udbydes tjenester i EU, er, at hostingstjenesteyderen gør det muligt for juridiske eller fysiske personer i en eller flere medlemsstater at gøre brug af tjenester fra hostingtjenesteyderen. Den blotte kendsgerning, at en tjenesteyders websted, e-mailadresse eller andre kontaktoplysninger kan tilgås i en eller flere medlemsstater, er dog isoleret set ikke tilstrækkeligt. Der stilles således krav om en "væsentlig tilknytning" til den eller de medlemsstater, hvor tjenesterne stilles til rådighed, hvilket vil skulle afgøres på grundlag af en række momenter. En sådan væsentlig tilknytning anses for at være til stede, hvis hostingtjenesteyderen er etableret i EU. For hostingtjenesteydere uden for EU vil det være afgørende, om der er et betydeligt antal brugere i en eller flere medlemsstater, eller om tjenesteudbyderen målretter sine tjenester en eller flere medlemsstater, f.eks. ved at markedsføre tjenesterne og varetage kundeservicen på den pågældende medlemsstats sprog, eller ved at udbyde apps i nationale appbutikker.

Hostingtjenesteydere er forpligtet til at etablere kontaktpunkter, enten internt eller outsourcet, som gør det muligt at modtage og hurtigt behandle påbud om fjernelse og indberetninger ad elektronisk vej.

Derudover er hostingtjenesteydere, som ikke er etableret i EU, men som udbyder sine tjenester i Unionen, forpligtet til skriftligt at udpege en juridisk

eller fysisk person som sin retlige repræsentant i Unionen med henblik på modtagelse, overholdelse og håndhævelse af påbud om fjernelse, indberetninger, anmodninger og afgørelser udstedt af de kompetente myndigheder. Den retlige repræsentant skal være bosiddende eller etableret i en af de medlemsstater, hvor hostingtjenesteyderen udbyder tjenester, og repræsentanten kan drages til ansvar for manglende overholdelse af forordningens bestemmelser, uden at det berører hostingtjenesteyderens ansvar og de søgsmål, der vil kunne anlægges over for denne.

Kompetente nationale myndigheder
Hver medlemsstat skal udpege den eller de nationale myndigheder, der skal varetage forpligtelserne i henhold til forordningen, herunder at:

a) udstede påbud om fjernelse
b) spore og identificere terrorindhold og indberette indholdet til hostingtjenesteyderne
c) føre tilsyn med gennemførelsen af proaktive foranstaltninger
d) håndhæve forpligtelserne i henhold til denne forordning ved hjælp af sanktioner

Medlemsstaterne kan ved udpegelsen af den eller de kompetente myndigheder frit vælge den eller de administrative, retshåndhævende eller retlige myndigheder, som de ønsker skal varetage ovenstående opgaver.

Rettidig omhu
For at skabe klarhed over det ansvar, der påhviler hostingtjenesteydere, har alle hostingtjenesteydere pligt til at træffe passende, rimelige og forholdsmæssige foranstaltninger under hensyntagen til ytrings- og informationsfriheden med henblik på at sikre, at deres platforme ikke misbruges til at udbrede terrorrelateret indhold. Denne omhu indebærer ikke en generel forpligtelse til overvågning.

Den rettidige omhu indebærer dog, at hostingtjenesteyderne skal handle på en omhyggelig, forholdsmæssig og ikke-diskriminerende måde i respekt for det indhold, de lagrer, navnlig når de gennemfører deres egne vilkår og betingelser, med henblik på at undgå fjernelse af indhold, som ikke er terrorindhold.

Pålæg om fjernelse af terrorrelateret indhold

En kompetent national myndighed, der kan være både administrativ og retlig, kan give hostingtjenesteydere påbud om at fjerne terrorrelateret indhold på deres platforme eller deaktivere adgangen til sådant materiale.

Hostingtjenesteyderen skal i givet fald fjerne eller deaktivere adgangen til det pågældende materiale inden for en time efter modtagelse af et påbud om fjernelse. Et påbud skal udformes på en formular, der er indsat som bilag til forslaget, og indeholde en række nærmere definerede oplysninger, herunder bl.a. en vurdering af indholdet med henvisning til, hvilken type terrorrelateret indhold der er tale om, og oplysninger om hostingtjenesteyderens og den pågældende indholdsleverandørs klagemuligheder.

På anmodning fra hostingtjenesteyderen eller indholdsleverandøren skal den kompetente myndighed give en supplerende forklaring på, hvorfor det pågældende indhold betragtes som terrorrelateret. Hostingtjenesteyderen er på trods af anmodningen stadig forpligtet til at fjerne indholdet inden for en time efter modtagelse af påbuddet.

Hostingtjenesteyderen skal anerkende modtagelsen af et påbud uden unødig forsinkelse. Ved hjælp af en formular, der er indsat som bilag til forslaget, skal hostingtjenesteyderen underette om, at det terrorelaterede indhold er blevet fjernet, eller at adgangen til indholdet er blevet deaktiveret samt tidspunktet for dette.

Indberetninger

Den kompetente nationale myndighed eller det relevante EU-organ, f.eks. Europol, kan sende en indberetning til en hostingtjenesteyder om oplysninger, som efter den pågældende myndigheds vurdering kan betragtes som terrorindhold, med henblik på, at hostingtjenesteyderen på frivillig basis overvejer, hvorvidt indholdet er i overensstemmelse med leverandørens egne vilkår og betingelser. Hostingtjenesteyderen skal uden unødig forsinkelse underrette den nationale kompetente myndighed eller det relevante EU-organ om resultatet af sine overvejelser, herunder eventuelle foranstaltninger, der træffes som følge af indberetningen, og tidsplanen herfor.

Proaktive foranstaltninger

Hostingstjenesteyderne skal, afhængig af risikoen og graden af eksponering for terrorrelateret indhold, iværksætte passende proaktive foranstaltninger for at beskytte deres tjenester mod udbredelsen af terrorrelateret indhold.

Har hostingtjenesteyderen ikke modtaget påbud om fjernelse og indberetninger, vil det være tegn på lav eksponering for terrorindhold. Kravet om proaktive foranstaltninger må ikke indebære en generel forpligtelse til overvågning.

Hvis en kompetent national myndighed har modtaget underretning om, at der over for en hostingtjenesteyder, som har hovedsæde eller en retlig repræsentant bosiddende eller etableret i medlemsstaten, er udstedt påbud om fjernelse af terrorrelateret indhold, skal den anmode hostingtjenesteyderen om inden for tre måneder og derefter mindst én gang årligt at fremlægge en rapport om de specifikke proaktive foranstaltninger, som den pågældende hostingtjenesteyder har iværksat for dels effektivt at forebygge, at terrorrelateret indhold, der er blevet fjernet, eller hvortil adgangen er blevet deaktiveret, bliver vist igen, dels at spore, identificere og hurtigt fjerne eller deaktivere adgangen til andet terrorrelateret indhold.

Mener den kompetente myndighed, at de proaktive foranstaltninger, som hostingtjenesteyderen har iværksat, er utilstrækkelige, kan den anmode udbyderen om at træffe yderligere proaktive foranstaltninger. Hostingtjenesteyderen skal i den forbindelse samarbejde med den kompetente myndighed om at indkredse, hvilke specifikke foranstaltninger som skal iværksættes.

Lykkes det ikke inden for en periode på 3 måneder for hostingtjenesteyderen og den kompetente myndighed at nå til en aftale om, hvilke specifikke proaktive foranstaltninger der skal iværksættes, kan den kompetente myndighed udstede en afgørelse, som pålægger hostingtjeneyderen at træffe særlige yderligere nødvendige og forholdsmæssige proaktive foranstaltninger. I en sådan afgørelse tages der bl.a. højde for især hostingtjenesteyderens økonomiske kapacitet, antallet af påbud om fjernelse og indberetninger og virkningen af sådanne foranstaltninger for brugernes grundlæggende rettigheder og den grundlæggende betydning af ytrings- og informationsfriheden. Den kompetente myndighed har i den forbindelse beføjelse til skønsmæssigt og i overensstemmelse med forordningens formål at fastsætte arten og omfanget af de proaktive foranstaltninger, der skal iværksættes.

Hostingtjenesteyderen kan til enhver tid anmode den kompetente myndighed om at tage anmodninger eller afgørelser om foranstaltninger op til revision og, hvis det er passende, tilbagekalde dem.

Sikkerhedsforanstaltninger og klagemekanismer

Hostingtjenesteydere, som anvender automatiserede værktøjer, skal have effektive og passende beskyttelsesforanstaltninger, som sikrer, at beslutninger navnlig vedrørende fjernelse eller deaktivering af adgangen til indhold, som anses for ulovligt indhold, er korrekte og velfunderede.

Derudover har hostingtjenesteydere pligt til at indføre effektive og tilgængelige klagemekanismer, som gør det muligt for indholdsleverandører, hvis indhold er blevet fjernet, eller hvor adgangen til indholdet er blevet deaktiviteret som følge af en indberetning eller proaktive foranstaltninger, at indgive en klage mod hostingtjenesteyderens handlinger.

Hostingtjenesteydere skal straks undersøge enhver klage, som modtages, og genindsætte indholdet uden unødig forsinkelse, hvis det uberettiget er blevet fjernet eller deaktiveret, og underrette klageren om udfaldet af undersøgelsen.

Samarbejde og jurisdiktioner
Den medlemsstat, hvor hostingtjenesteyderens hovedsæde befinder sig, har jurisdiktion med henblik på anmodninger og afgørelser om proaktive foranstaltninger, økonomiske sanktioner og overvågning. En hostingtjenesteyder, hvis hovedsæde ikke befinder sig i en medlemsstat, anses for at høre under den medlemsstats jurisdiktion, hvor den af hostingtjenesteyderen udpegede retlige repræsentant er bosiddende eller etableret. Enhver medlemsstat har jurisdiktion, for så vidt angår påbud om fjernelse og indberetninger, uanset hvor den pågældende hostingtjenesteyder har sit hovedsæde eller har udpeget en retligt repræsentant.

Hvis en hostingtjenesteyder ikke udpeger en retlig repræsentant, har alle medlemsstater kompetence. Hvis en medlemsstat beslutter at udøve sin jurisdiktion, skal medlemsstaten informere samtlige medlemsstater herom.
De kompetente myndigheder i medlemsstaterne skal informere, koordinere og samarbejde med hinanden og om nødvendigt med relevante kompetente EU-organer såsom Europol med hensyn til påbud om fjernelse og indberetninger for at undgå dobbeltarbejde, øge koordineringen og undgå forstyrrelser af efterforskninger i forskellige medlemsstater. Det indebærer bl.a., at de kompetente myndigheder i medlemsstaterne skal informere, koordinere og samarbejde med den kompetente myndighed, som har jurisdiktion til at fastsætte proaktive foranstaltninger og sanktioner for en given hostingtjenesteyder. Medlemsstaterne sikrer i den forbindelse, at den pågældende kompetente myndighed er i besiddelse af alle relevante oplysninger ved bl.a. at

tilvejebringe passende kommunikationskanaler eller -mekanismer, som sikrer rettidig deling af relevante oplysninger.

Hvis en hostingtjenesteyder bliver bekendt med beviser for terrorhandlinger, skal den omgående informere de myndigheder, der er kompetente til at efterforske og retsforfølge strafbare handlinger i den eller de berørte medlemsstater. Hvis det er umuligt at identificere den eller de pågældende medlemsstater, underretter hostingtjenesteyderen de relevante myndigheder i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde eller har udpeget en retlig repræsentant, og videregiver også oplysningerne til Europol.

Sanktioner

Medlemsstaterne skal fastsætte regler vedrørende økonomiske sanktioner i tilfælde af en hostingtjenesteyders overtrædelse af forordningens bestemmelser om hostingtjensteyders vilkår og betingelser, gennemførelse af og feedback om påbud om fjernelse, vurdering af og fedback af indberetninger, pligt til rapportering om proaktive foranstaltninger mv., opbevaring af data, pligt til gennemsigtighed, pligt til at træffe sikkerhedsforanstaltninger vedrørende proaktive foranstaltninger og klageprocedurer, oplysninger til indholdsleverandører, oplysninger om beviser på terrorhandlinger, kravet om kontaktpunkter og udpegelse af en retlig repræsentant.

Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. I den forbindelse skal medlemsstaterne sikre, at de kompetente myndigheder ved fastsættelse af sanktionernes art og størrelse tager hensyn til følgende relevante omstændigheder:

(6) Overtrædelsens art, grovhed og varighed
(7) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt
(8) overtrædelser, som den juridiske eller fysiske person, der er ansvarlig for overtrædelsen, tidligere har begået
(9) den ansvarlige juridiske eller fysiske persons finansielle styrke
(10) hostingtjenesteyderens grad af samarbejde med de kompetente myndigheder

Derudover skal medlemstaterne sikre, at systematisk mangel på overholdelse af forpligtelsen til at fjerne eller deaktivere terrorrelateret indhold inden for en time efter at have modtaget påbuddet om fjernelse af en kompetent national myndighed medfører økonomiske sanktioner på op

til 4 pct. af hostingtjenesteyderens samlede omsætning for det seneste regnskabsår.

På rådsmødet (retlige og indre anliggender) den 14. december 2020 forventes formandskabet at orientere om status for trilogforhandlingerne om forslaget og om en eventuel foreløbige aftale, der på tidspunktet for rådsmødet måtte være indgået med Europa-Parlamentet.

4. Europa-Parlamentets udtalelser

Forslaget til forordning om forebyggelse af udbredelsen af terrorrelateret online-indhold behandles efter den almindelige lovgivningsprocedure (TEUF artikel 294), der indebærer, at forslaget skal vedtages med Europa-Parlamentet som medlovgiver.

Forslaget behandles i Europa-Parlaments Udvalg for Borgernes Rettigheder og Retlige og Indre Anliggender (LIBE).

Europa-Parlamentet afsluttede førstelæsningen af forslaget den 17. april 2019 med vedtagelsen af en udvalgsbetænkning fra LIBE-udvalget med stemmerne 308 for, 204 imod og 70 hverken for eller imod. I udvalgsbetænkningen har LIBE-udvalget fremsat en række ændringsforslag til forordningsforslaget.

Bl.a. foreslår udvalget, at forordningen ikke skal finde anvendelse for indhold, der udbredes i undervisningsmæssig, kunstnerisk, journalistisk eller forskningsmæssig øjemed eller med henblik på at skabe fokus på terrorelaterede aktiviteter eller som repræsenterer kontroversielle synspunkter som en del af en offentlig debat.

Herudover foreslår udvalget, at hvis den kompetente myndighed ikke tidligere har sendt et påbud til en hostingtjenesteyder, skal den kompetente myndighed kontakte hostingstjenesteyderen 12 timer før, at et påbud udstedes. Det foreslås, at påbuddet skal indeholde en detaljeret redegørelse for, hvorfor indholdet er terrorrelateret.

Endvidere foreslås det, at forordningsforslaget ikke skal indeholde en adgang til at sende indberetninger til hostingstjenesteydere.

Udvalget foreslår bl.a. også, at hostingtjenesteydere ikke skal forpligtes til at iværskætte proaktive foranstaltninger, men at en hostingtjenesteyder, der har modtaget et betydeligt antal påbud, kan blive anmodet om at iværksætte

nødvendige, proportionale og effektive foranstaltninger af den kompetente myndighed.

I forhold til jurisdiktion mener udvalget ikke, at enhver medlemsstat skal have kompetence til at udstede et påbud om fjernelse til en hostingtjenestyder. Udvalget foreslår, at den kompetente myndighed i den medlemsstat, hvor hostingtjenesteyderen har sit hovedsæde, skal have kompetencen til at udstede et påbud om, at hostingtjenesteyderen skal fjerne eller deaktivere adgangen til terrorrelateret indhold i alle medlemsstater.

I forhold til udvælgelse af en kompetent myndighed har udvalget foreslået, at myndigheden skal være en retslig myndighed eller en funktionelt uafhængig administrativ myndighed.

Det bemærkes, at forslaget som nævnt aktuelt fortsat er under trilogforhandling, og at der løbende fremsættes kompromisforslag.

5. Nærhedsprincippet

Kommissionen har anført, at internettet i sagens natur er grænseoverskridende, og at indhold, der hostes i en medlemsstat, normalt kan tilgås fra enhver anden medlemsstat. Kommissionen anfører, at denne grænseoverskridende dimension nødvendiggør tiltag på EU-niveau for at opnå de fastsatte mål.

Kommissionen har i den forbindelse anført, at forskellige nationale regler til bekæmpelse af terrorrelateret onlineindhold resulterer i en fragmenteret ramme, som kan pålægge virksomhederne en byrde, fordi de skal overholde forskellige regler, ligesom det skaber ulige vilkår for virksomhederne og sikkerhedsmæssige smuthuller.

Kommissionen anfører derfor, at forslaget skal højne retssikkerheden og øge effektiviteten af hostingtjenesteydernes indsats for at bekæmpe terrorrelateret onlineindhold.

På baggrund af det grænseoverskridende element, de forskellige nationale regler i medlemsstaterne til bekæmpelse af terrorrelateret onlineindhold og hensynet til de berørte virksomheders retssikkerhed, vurderer Kommissionen således, at det er berettiget med lovgivning på EU-niveau for at kunne adressere de angivne problemer.

Kommissionens vurdering støttes ligeledes af DER-konklusioner af 28. juni 2018, hvor Kommissionen opfordredes til at fremlægge et lovgivningsforslag på området.

Forslaget vurderes – af de af Kommissionen anførte grunde – at være i overensstemmelse med nærhedsprincippet.

6. Gældende dansk ret

Det følger af grundlovens § 77, at enhver er berettiget til på tryk, i skrift og tale at offentliggøre sine tanker, dog under ansvar for domstolene, og at censur og andre forebyggende forholdsregler ingensinde på ny kan indføres.

Grundloven beskytter den såkaldte formelle ytringsfrihed. Det vil sige, at den beskytter retten til at udtale sig uden forudgående kontrol. Bestemmelsen omfatter egentlig censur, hvor en offentlig myndighed skal godkende en ytring, før den offentliggøres. Den omfatter også censurlignende foranstaltninger, der kan hindre eller forsinke offentliggørelsen af ytringer.

Grundlovens § 77 er dog ikke til hinder for, at domstolene kan nedlægge forbud mod, at ikke offentliggjorte ytringer bliver offentliggjort.

Efter dansk statsret anses danske myndigheder som udgangspunkt for at være enekompetente til at udøve myndighedsbeføjelser inden for det danske territorium (det såkaldte uskrevne grundlovsforbud). Som en undtagelse hertil følger det af grundlovens § 20, at de beføjelser, som efter grundloven tilkommer rigets myndigheder, ved lov i nærmere bestemt omfang kan overlades til mellemfolkelige myndigheder som f.eks. EU. Bestemmelsen giver derimod ikke adgang til at overlade beføjelser til andre stater.

Danmark har i regi af den nationale handlingsplan om forebyggelse og bekæmpelse af ekstremisme og radikalisering fra oktober 2016 gennemført en række tiltag, der har til formål at bekæmpe ekstremistisk propaganda og forebygge online-radikalisering, bl.a. ved at fjerne og blokere terrorrelateret indhold på internettet.

Der blev således i sommeren 2017 på initiativ fra *den daværende* regering indsat en ny bestemmelse i retsplejelovens § 791 d, der giver hjemmel til at blokere en hjemmeside, hvis der er rimelig grund til at antage, at der fra hjemmesiden begås en overtrædelse af bl.a. straffelovens §§ 114-114 i om terrorisme. Afgørelser om blokering af en hjemmeside træffes ved retskendelse efter begæring fra politiet.

Derudover har Danmark ligesom en række andre medlemsstater i regi af EU's Internetforum etableret en såkaldt internet referral unit (IRU-enhed), der er forankret i Politiets Efterretningstjeneste (PET). Enheden har til formål at identificere voldeligt ekstremistisk indhold på nettet, herunder terrorrelateret indhold, og indberette indholdet til hostingtjenesteydere med henblik på hurtig fjernelse. Enheden indgår ligeledes i et samarbejde med Europol med henblik på at koordinere bortfjernelse af terrorrelateret materiale.

7. Konsekvenser

Lovgivningsmæssige konsekvenser

En forordning er umiddelbart bindende i alle enkeltheder og gælder umiddelbart i hvert EU-medlemsland.

Forslaget forventes dog alligevel at have lovgivningsmæssige konsekvenser, da det bl.a. vil være nødvendigt at fastsætte regler om, hvilken national myndighed der skal kunne udstede påbud til hostingtjenesteydere om fjernelse af terrorrelateret indhold, og hvilken myndighed der skal kunne pålægge en hostingtjenesteyder at iværksætte proaktive foranstaltninger.

Økonomiske konsekvenser

Vurderingen af, hvorvidt forslaget vil have statsfinansielle konsekvenser, er endnu ikke afsluttet. Det vurderes dog ikke umiddelbart, at forslaget vil have statsfinansielle konsekvenser af betydning.

Det vurderes umiddelbart, at forslaget kan medføre administrative byrder under 4 mio. kr. årligt som følge af krav til hostingtjenesteyderne om oplysninger til brugere samt om fjernelse eller deaktivering af terrorrelateret onlineindhold. Ud over de administrative konsekvenser kan forslaget medføre væsentlige erhvervsøkonomiske konsekvenser som følge af forslagets bestemmelser om pligt for hostingtjenesteydere til efter påbud at fjerne terrorrelateret indhold inden for en time, indberetning og proaktive foranstaltninger. Den endelig vurdering heraf er dog endnu ikke afsluttet.

8. Høring

Der er foretaget høring af Specialudvalget for politimæssigt og retligt samarbejde den 2. og 21. november 2018 i sagen.

Kommissionens forslag har tidligere været sendt i høring hos følgende myndigheder og organisationer mv.:

Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Præsidenten for Sø- og Handelsretten, Præsidenterne for byretterne, Den Danske Dommerforening, Dommerfuldmægtigforeningen, Domstolsstyrelsen, Dansk Erhverv, Dansk Industri, Danske Medier, Datatilsynet, DK Hostmaster, Fiberby, Institut for Menneskerettigheder, IT-Politisk Forening, Justitia Kriminalpolitisk Forening (KRIM), Rigsadvokaten, Teleindustrien, Telia Danmark, Københavns Universitet, Syddansk Universitet (Juridisk Institut), Aalborg Universitet (Juridisk Institut), Aarhus Universitet (Juridisk Institut) og Danmarks Tekniske Universitet.

Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Præsidenten for Sø- og Handelsretten, Domstolsstyrelsen og Datatilsynet har afgivet høringssvar, men har ikke haft bemærkninger til forslaget.

Dansk Erhverv, Dansk Industri, Institut for Menneskerettigheder og IT-Politisk Forening har den 21. november 2018 afgivet høringssvar med bemærkninger til forslaget.

Dansk Erhverv (DE) udtrykker sig kritisk over for forslaget. DE anfører i den forbindelse, at forslaget giver anledning til retssikkerhedsmæssige overvejelser. DE udtrykker samtidig bekymring for de byrder, som forslaget pålægger danske virksomheder. DE anerkender dog, at bekæmpelse af terror er et politisk tema, som kræver internationale svar.

DE finder, at definitionen af hostingtjenesteydere er uklar og potentielt omfatter alt fra sociale medier, hobby og debatfora til udbydere af webhosting, cloud-løsninger og datacentre. De to sidstnævnte udlejer kapacitet og har ikke nødvendigvis adgang til de it-systemer og data, der afvikles eller lagres på deres infrastruktur, og vil derfor ikke umiddelbart have adgang til at nedtage eventuelt terrorrelateret indhold.

DE bemærker endvidere, at definitionen af terrorrelateret indhold er bred og kan omfatte en meget bred vifte af indholdstyper. DE finder det endvidere betænkeligt, at der med forslaget åbnes op for administrative påbud. DE anbefaler i den forbindelse, at påbud pålægges ved en retskendelse.

For så vidt angår den del af forslaget, der omhandler sanktioner, påpeger DE, at forslaget indeholder en meget uklar definition af, hvornår der er tale om systematisk mangel på overholdelse af forpligtelserne i artikel 4, stk. 2, som medfører økonomiske sanktioner på op til 4 pct. af omsætningen. DE henstiller i den forbindelse til, at dette afklares.

Dansk Industri (DI) støtter formålet med forordningsforslaget om at skabe en klar og harmoniseret retlig europæisk ramme til at forebygge, at hostingtjenester misbruges til at få udbredt terrorrelateret indhold på internettet.

DI bemærker, at definitionen af hostingtjenesteydere er meget bred og uklar, og at det er vigtigt at afklare sammenhængen med reglerne i e-handelsdirektivet, så der ikke opstår tvivl om, hvilke regler der gælder. DI opfordrer desuden til, at det præciseres, at mails og cloud-tjenester mv. kun er omfattet af forslaget i de tilfælde, hvor der er en reel konkret risiko for udbredelse af terrorrelateret indhold.

Vedrørende definitionen af terrorrelateret indhold bemærker DI, at den er bredt formuleret og kan omfatte mange former for indhold, hvilket kan gøre det svært for virksomhederne. DI anbefaler derfor, at definitionen henviser til den liste over personer, grupper og enheder, som EU og FN fører, så der ikke opstår tvivl om, hvem der er omfattet.

DI anfører endvidere, at et påbud om fjernelse af terrorrelateret indhold bør udstedes i henhold til en retskendelse. Samtidig bør myndighederne være forpligtet til altid at fremsende en detaljeret begrundelse, så hostingtjenesteyderen kan foretage en konkret vurdering af et påbud, før indholdet fjernes fra internettet. I modsat fald kan der være risiko for, at hostingtjenesteyderen fjerner indholdet uden at foretage sig yderligere, hvilket kan give problemer i forhold til ytringsfriheden.

For så vidt angår iværksættelse af proaktive foranstaltninger bemærker DI, at forslaget potentielt ændrer ved e-handelsdirektivets grundlæggende mekanismer for ansvarsfritagelse. Forslaget tillader endda, at myndighederne fastsætter krav til, hvilke tekniske tiltag en virksomhed bør gennemføre. DI finder, at dette kan bremse virksomheders egen teknologiske udvikling og holde dem fra at skabe nye smarte digitale løsninger, og at bestemmelsen bør præciseres, så virksomhederne tilskyndes til selv at finde på nye effektive og innovative løsninger til at takle udbredelse af terrorrelateret onlineindhold.

DI finder endelig, at den høje bødestraf på op til 4 pct. af omsætningen kun bør gælde ved de mest alvorlige overtrædelser, hvor en hostingtjenesteyder handler groft uagtsomt eller direkte i ond tro. DI anfører, at oprettelsen af

en central europæisk enhed eller agentur kan bidrage til at sikre større ensartethed for bødeniveauet på tværs af medlemsstater og understøtte god udveksling af erfaringer, best practice mv.

Institut for Menneskerettigheder (IMR) bemærker, at forslaget regulerer et væsentligt og legitimt formål om terrorbekæmpelse. Forslaget indebærer dog, at der foretages indgreb i ytringsfriheden, som er beskyttet bl.a. i EU-Chartrets artikel 11 og Den Europæiske Menneskerettighedskonventions artikel 10.

IMR bemærker i den forbindelse, at adgangen til at meddele påbud om fjernelse af terrorrelateret materiale efter IMR's vurdering som udgangspunkt vil være omfattet af adgangen til at gøre indgreb i ytringsfriheden efter artikel 10, stk. 2, hvis ikke indholdet er helt uden for beskyttelsesområdet, jf. artikel 17.

IMR finder det imidlertid ikke godtgjort, at adgangen til at indgive indberetning til hostingtjenesteydere er et proportionalt indgreb i ytringsfriheden. IMR peger i den forbindelse på, at staten har en positiv forpligtelse til at sikre ytringsfriheden, at indberetningerne foretages i de tilfælde, hvor myndigheden ikke selv har fundet/kan finde juridisk grundlag for at nedlægge påbud om fjernelse af indholdet, at hostingtjenesteyderne ikke skal foretage en vurdering af indholdet i forhold til forordningen, men derimod deres egne vilkår og betingelser, at hostingtjenesteydernes stillingtagen til indberetningerne er sanktionsbelagt, og at indberetningerne kan medføre, at hostingtjenesteyderne og indholdsleverandøren ud fra et forsigtighedsprincip i højere grad, end hvad der er nødvendigt, vil begrænse materiale og indhold. IMR anbefaler derfor, at bestemmelserne om indberetning udgår af forslaget, eller at bestemmelserne ændres, så hostingtjenesteydernes stillingtagen til indberetningerne ikke er strafbelagt.

For så vidt angår de dele af forslaget, der vedrører hostingtjenesteyderens pligt til at gennemføre passende foranstaltninger, bemærker IMR, at der er visse retssikkerhedsmæssige bekymringer ved brugen af uploadfiltre. På grund af risikoen for uproportionale indgreb i ytringsfriheden anbefaler IMR derfor, at adgangen til brug af uploadfiltre udgår fra forordningen. Hvis adgangen til brug af uploadfiltre ikke udgår af forslaget, anbefaler IMR, at der i forslaget redegøres nøje for, hvordan man vil imødegå risikoen for manglende proportionalitet og dermed risikoen for krænkelse af ytringsfriheden ved anvendelsen af uploadfiltre.

Vedrørende adgangen for de kompetente myndigheder til at træffe afgørelse om proaktive foranstaltninger bemærker IMR, at det bør fremgå af forslaget, at en afgørelse om specifikke proaktive foranstaltninger ikke fører til en generel forpligtelse til overvågning, idet en generel forpligtelse til overvågning vil være et indgreb i retten til respekt for privatliv, som er beskyttet i bl.a. Chartrets artikel 7 og Den Europæiske Menneskerettighedskonventions artikel 8. I lyset af bl.a. praksis fra EU-Domstolen finder IMR, at adgangen til generel overvågning ikke er tilstrækkeligt godtgjort som et proportionalt indgreb i retten til respekt for privatlivet, navnlig fordi det ikke er sandsynliggjort, at formålet ikke kan varetages med en mindre indgribende foranstaltning end brugen af uploadfiltre.

IT-Politisk Forening (IPF) finder forordningsforslaget meget problematisk, fordi det åbner op for en ret vidtgående censur af borgernes ytringer på internettet samt en automatiseret overvågning af disse ytringer.

Vedrørende definitionen af terrorrelateret indhold bemærker IPF, at den rækker langt ud over indhold, som opfordrer til udførelse af terrorhandlinger, og som kan udgøre en reel fare for den offentlige sikkerhed. IPF anbefaler derfor, at forslaget ændres, så det alene omfatter indhold, som direkte opfordrer til udførelse af terrorhandlinger.

For så vidt angår definitionen af hostingtjenesteydere bemærker IPF, at der er tale om en meget bred definition, som omfatter enhver informationssamfundstjeneste, der tillader brugerne at lagre indhold og stille det til rådighed for tredjeparter. IPF anfører, at der er behov for en mere præcis og snæver definition af hostingtjenesteydere i forslaget, hvori det bl.a. præciseres, at udbydere af elektroniske kommunikationstjenester ikke er omfattet. IPF bemærker i forlængelse heraf, at der ikke er proportionalitet mellem det, man ønsker at opnå med forordningen, og de økonomiske og praktiske byrder, som forslaget pålægger især små og mellemstore virksomheder. En forventelig konsekvens af forslaget vil være, at mange små informationssamfundstjenester med brugergenereret indhold vil lukke eller vil outsource funktionaliteten med brugergenereret indhold til store virksomheder som f.eks. Facebook. IPF anbefaler derfor, at der i forordningsforslaget indføres en passende undtagelse for små hostingtjenesteydere.

IPF peger endvidere på, at det følger af forslaget, at en dansk hostingtjenesteyder kan modtage påbud om fjernelse af terrorrelateret indhold fra både en dansk kompetent myndighed og fra kompetente myndigheder i andre EU-

lande. Det indebærer i praksis en gensidig anerkendelse mellem EU-medlemsstater af kompetente myndigheder, der kan udstede påbud om fjernelse af indhold.

IPF anfører i forlængelse heraf, at hvis en hostingtjenesteyder eller indholdsleverandør vil gøre indsigelse mod et påbud, skal denne indsigelse ske til domstolene i den medlemsstat, hvis kompetente myndighed har udstedt påbuddet. Adgangen til at gøre indsigelse vil være uforholdsmæssig vanskelig, hvis et påbud kan udstedes på tværs af landegrænser. IPF anbefaler derfor, at forslaget ændres, så påbud om fjernelse alene kan udstedes af de kompetente myndigheder i den medlemsstat, hvor hostingtjenesteyderen er etableret eller repræsenteret.

I den forbindelse bemærker IPF, at hvis påbud om fjernelse af indhold i Danmark alene kan udstedes af en domstol, kan denne beskyttelse af retssikkerheden i praksis blive undergravet af andre EU-medlemsstater, som tillader administrative myndigheder at udstede påbud, idet alle kompetente myndigheder efter forslaget kan udstede påbud i alle EU-medlemsstater. IPF anbefaler, at forslaget ændres, så der stilles krav til medlemsstaterne om, at den kompetente myndighed skal være en domstol eller i det mindste en uafhængig administrativ myndighed.

IPF finder det desuden uhensigtsmæssigt, at den kompetente myndighed kan vælge mellem at udstede et påbud om fjernelse af terrorrelateret indhold eller sende en indberetninger til hostingtjenesteyderen, idet det herved kan blive overladt til virksomhederne at tage stilling til de svære tilfælde, hvor det pågældende indhold ligger i en gråzone.

IPF påpeger, at forslaget ikke indeholder en reel definition af, hvad der skal forstås ved proaktive foranstaltninger, men at forslagets artikel 6, stk. 2, antyder, at der kan være tale om automatiserede værktøjer (automatisk indholdsfiltrering) med henblik på at forhindre gen-upload af allerede identificeret terrorrelateret indhold og spore, identificere og hurtigt fjerne terrorrelateret indhold, som ikke på forhånd er kendt.

IPF anfører i den forbindelse, at proaktive foranstaltninger, som har til formål at identificere ukendt terrorrelateret indhold, vil indebærer en stor risiko for overblokering, dvs. at lovligt indhold fejlagtigt identificeres som terrorrelateret og fjernes af automatiske algoritmer. Staten bør ikke kunne pålægge private virksomheder at indføre sådanne foranstaltninger, når staten ikke kan garantere, at disse foranstaltninger ikke har negativ indvirkning på

borgernes grundlæggende rettigheder, herunder ytrings- og informationsfriheden samt retten til privatliv og beskyttelse af personlige oplysninger. Hertil kommer, at generelle proaktive foranstaltninger rettet mod fremtidigt ukendt terrorrelateret indhold vil kunne udgøre egentlig forhåndscensur i forhold til grundlovens § 77.

Teleindustrien tilslutter sig høringssvarene fra Dansk Erhverv og Dansk Industri. Derudover fremhæver Teleindustrien, at det er vigtigt, at det er en domstol, som tager stilling til, om konkret indhold på nettet skal fjernes.

Teleindustrien anfører desuden, at forslagets artikel 5 og 6 om indberetninger og fastsættelse af proaktive foranstaltninger vil indebære, at private aktører bliver pålagt et ansvar for at identificere og vurdere specifikt indhold på nettet og tage stilling til, om det skal fjernes. Teleindustrien finder, at en sådan vurdering og beslutning alene bør foretages af domstolene.

9. Generelle forventninger til andre landes holdninger

Som det fremgår af afsnit 2 ovenfor, fremlagde Frankrig og Tyskland den 19. juni 2018 en erklæring om fremtidige tiltag i EU, hvori de to lande bl.a. opfordrede til indførelse af lovgivning på EU-niveau for at bekæmpe terrorrelateret indhold på nettet.

På rådsmødet (retlige og indre anliggender) den 6.-7. december 2018 vedtog Rådet sin generelle indstilling til forslaget. Fire medlemslande, herunder Danmark, stemte imod vedtagelsen.

10. Regeringens generelle holdning

Fra dansk side har man overordnet set været positivt indstillet over for forordningsforslaget, herunder formandskabets kompromisforslag, der har til formål at styrke og supplere den fælles og frivillige indsats, der allerede er iværksat på EU-niveau i forhold til at bekæmpe mængden af terrorrelateret indhold på nettet. Forslaget kan samtidig styrke og supplere den indsats for bekæmpelse af terrorrelateret indhold på nettet, som er iværksat på nationalt plan.

Derved kan forordningsforslaget udgøre et effektivt redskab i kampen mod terrorisme.

Det er imidlertid vurderingen, at bestemmelserne om jurisdiktion til at udstede påbud og indberetninger, herunder artikel 15, i Rådets generelle indstilling til forslaget rejser spørgsmål i forhold til grundloven (det såkaldte uskrevne grundlovsforbud).

Bestemmelserne om jurisdiktion indebærer, at en kompetent myndighed i en anden medlemsstat kan træffe en retligt bindende afgørelse i form af f.eks. et påbud om fjernelse af terrorrelateret indhold over for en hostingtjenesteyder i Danmark. Afgørelsen bliver bindende for hostingtjenesteyderen umiddelbart og uden, at en dansk myndighed bliver involveret først.

Efter statsretten anses danske myndigheder som udgangspunkt for at være enekompetente til at udøve myndighedsbeføjelser inden for det danske territorium (det såkaldte uskrevne grundlovsforbud). Som en undtagelse hertil følger det af grundlovens § 20, at de beføjelser, som efter grundloven tilkommer rigets myndigheder, ved lov i nærmere bestemt omfang kan overlades til mellemfolkelige myndigheder som f.eks. EU. Bestemmelsen giver derimod ikke adgang til at overlade beføjelser til andre stater.

Fra dansk side tillægges det afgørende vægt, at problemet i forhold til det uskrevne grundlovsforbud bliver løst forud for forordningens eventuelle vedtagelse. Der arbejdes i den forbindelse for, at der opnås en enighed om en løsning, der tager højde for den særlige danske situation, ved at et påbud mv., inden det får virkning i Danmark, sendes til en kompetent dansk myndighed, som herefter øjeblikkeligt videresender det til hostingtjenesteudbyderen i Danmark. Herved kan det sikres, at en dansk myndighed involveres, før et påbud mv. får virkning i Danmark.

Herudover har man fra dansk side haft fokus på, at ordningen vedrørende pålæg om proaktive foranstaltninger kan gennemføres inden for rammerne af grundlovens § 77. Det vurderes at være tilfældet for så vidt angår den nu foreslåede ordning i Rådets generelle indstilling.

I forbindelse med de igangværende forhandlinger vil der fra dansk side fortsat være fokus på, at forordningen respekterer grundlovens § 77.

Om de proaktive foranstaltninger, som hostingtjenesteyderne af egen drift skal iværksætte, er det på nuværende tidspunkt uklart, hvad der nærmere skal forstås ved sådanne foranstaltninger. Det fremgår dog af Rådets generelle indstilling, at det er hostingtjenesteyderne, som skal beslutte, hvilke

hensigtsmæssige, effektive og proportionale foranstaltninger der skal iværksættes.

Fra dansk side vil man arbejde for, at der kommer klarhed over, at disse proaktive foranstaltninger ikke indebærer en pligt for hostingtjenesteyderne til at hindre eller forsinke offentliggørelsen af ytringer.

Man har fra dansk side endvidere haft fokus på at sikre, at forslaget ikke skaber urimelige eller uproportionale byrder for erhvervslivet, herunder navnlig små og mellemstore virksomheder, eller opstiller unødige barrierer for innovation og vækst i det digitale indre marked, ligesom at der skal tages højde for eksisterende krav i de gældende regler, så der sikres en klar, enkel og sammenhængende ramme for virksomhederne.

Det er i Rådets generelle indstilling blevet præciseret, at en hostingtjenesteyder kan outsource sit operationelle kontaktpunkt til en tredjemand, således at påbud om fjernelse og indberetninger nemmere og mere effektivt kan håndteres. Derudover har Kommissionen tilkendegivet, at Europol i forhold til iværksættelsen af proaktive foranstaltninger vil stille tekniske startpakker til rådighed for hostingtjenesteyderne med henblik på at styrke deres tjenesters modstandsdygtighed over for terrorrelateret indhold.

Det vurderes derfor fra dansk side, at Rådets generelle indstilling indebærer en fornuftig balance mellem på den ene side hensynet til hurtigt og effektivt at få fjernet terrorrelateret indhold på nettet og modvirke såkaldte "safe havens" på mindre platforme og på den anden side hensynet til byrderne for virksomhederne.

11. Tidligere forelæggelser for Folketingets Europaudvalg

Grund- og nærhedsnotat er fremsendt til Folketingets Europaudvalg den 5. november 2018.

Forordningsforslaget har været drøftet i Folketingets Europaudvalg den 9. november 2018 i forbindelse med justitsministerens besvarelse af samrådsspørgsmål B.

Sagen har været forelagt Folketingets Europaudvalg forud for rådsmødet (retlige og indre anliggender) den 6.-7. december 2018 med henblik på forhandlingsoplæg.

Sagen har været forelagt Folketingets Europaudvalg forud for rådsmødet (retlige og indre anliggender) den 2.-3. december 2019 til orientering.

Sagen har været forelagt Folketingets Europaudvalg forud for det ekstraordinære rådsmøde (retlige og indre anliggender) den 13. november 2020 til orientering.

Dagsordenspunkt 2: Konklusioner om intern sikkerhed og europæisk politipartnerskab/ andre forhold relateret til intern sikkerhed

Nyt notat.

Sagen er ikke omfattet af retsforbeholdet.

KOM-dokument foreligger ikke.

1. Resumé

Sagen er på dagsordenen for rådsmødet (retlige og indre anliggender) den 14. december 2020 med henblik på en politisk drøftelse. Med udgangspunkt i tidligere drøftelser under foregående formandskaber og Kommissionens offentliggørelse af strategien for EU's interne sikkerhed lægger det tyske formandskab op til lancering af et europæisk politipartnerskab. Der lægges med drøftelsen op til at udpege udvalgte milepæle, som suppleres af en række fokuspunkter, herunder styrkelse af EU-politisamarbejdet, anvendelse af teknologiske fremskridt, internationalt samarbejde, bekæmpelse af grænseoverskridende, organiseret kriminalitet og bekæmpelse af terror og politisk motiveret ekstremestisk vold. Sagen er ikke omfattet af retsforbeholdet. Spørgsmålet om nærhedsprincippet er ikke relevant. Sagen har hverken lovgivningsmæssige eller økonomiske konsekvenser. Man kan fra dansk side tage drøftelsen til efterretning.

2. Baggrund

Det daværende rumænske formandskab indledte i maj 2019 en debat om fremtiden for EU's interne sikkerhed. Under både det finske og det kroatiske formandskab blev der fulgt op på emnet, hvor man mere detaljeret søgte at beskrive fremtiden for EU's interne sikkerhed. Det tyske formandskab ønsker bl.a. i lyset heraf og med afsæt i lanceringen af strategien for EU's sikkerhedsunion i juli 2020 at bygge videre på dette arbejde og at lancere et europæisk politipartnerskab som ramme for perioden 2021-2025.

Det tyske formandskab fremhæver, at EU's område med frihed, sikkerhed og retfærdighed kræver et tæt samarbejde mellem alle retshåndhævende myndigheder, herunder særligt politimyndigheder. For yderligere at effektivisere EU's sikkerhedsarkitektur udpeges nogle overordnede milepæle, herunder at alle politibetjente på alle tidspunkter skal have adgang til den information, der er nødvendig for, at de kan gøre deres arbejde, og at med-

lemsstaterne og EU skal implementere tekniske løsninger for de retshåndhævende myndigheder, så de kan kommunikere sikkert og fortroligt i alle situationer. Milepælene suppleres af følgende fokuspunkter, som skal understøtte de udpegede milepæle for politisamarbejdet i perioden 2021-2015.

Styrkelse af det europæiske politisamarbejde gennem forbedring af samarbejdet mellem politimyndigheder på tværs af grænser. Europol, Frontex og eu-LISA fremhæves som hjørnesten i den europæiske sikkerhedsarkitektur, og der opfordres til at sikre passende midler og personale til disse agenturer.

Udnyttelse af de teknologiske fremskridt, herunder de retshåndhævende myndigheders brug af kunstig intelligens fremhæves også som fokuspunkt. Der er lagt op til, at brugen af kunstig intelligens potentielt kan facilitere og forbedre sikkerheden samt forebyggelsen, efterforskningen og retsforfølgelsen af kriminalitet i EU. Brugen af kunstig intelligens fremhæves som særlig relevant i forbindelse med cyberkriminalitet, seksuel udnyttelse af børn, narkotikakriminalitet og økonomisk kriminalitet. Det understreges, at anvendelsen af kunstig intelligens skal overholde grundlæggende rettigheder og databeskyttelsesregler.

Yderligere fremhæves det, at hybride trusler påvirker alle policy-sektorer, og at koordination mellem EU-institutionerne og medlemsstaterne derfor er nødvendig. Kommissionen opfordres til at vurdere udfordringer og risici for kriminelles anvendelse af kunstig intelligens i denne sammenhæng for derved at bistå EU og medlemslandene i at styrke de nationale modforanstaltninger. Om hybride trusler kan det fremhæves, at truslerne er mangeartede, kan komme fra såvel statslige og ikke-statslige aktører og vedrører både den eksterne og indre sikkerhed. Som eksempler på hybride trusler i relation til den indre sikkerhed kan nævnes bl.a. påvirkningskampagner og systematisk chikane af myndighedspersoner for at skabe mistillid til offentlige autoriteter. Hybride trusler er således flerdimensionelle og kombinerer tvangsforanstaltninger og undergravende foranstaltninger ved hjælp af både konventionelle og ukonventionelle værktøjer og taktikker (diplomatiske, militære, økonomiske og teknologiske) til at destabilisere modparten.

Endelig understreges det, at kryptering skal fremmes for at understøtte tiltroen til digitalisering, for at beskytte privatlivets fred mv., men at det samtidig er afgørende at beskytte retshåndhævende og retlige myndigheders mulighed for at løse deres opgaver. Ethvert tiltag skal således balancere disse hensyn nøje og foregå i tæt dialog med tech-industrien.

Fokuspunktet *"Globale udfordringer og internationalt samarbejde på sikkerhedsområdet"* lægger op til, at der skal være et samarbejde med strategiske tredjelande.

Bekæmpelse af grænseoverskridende organiseret kriminalitet fremhæves også som fokuspunkt, hvor der lægges op til, at særligt narkotikakriminalitet, seksuel udnyttelse af børn, handel med skydevåben og menneskehandel skal være i fokus.

For så vidt angår fokuspunktet "*Forebyggelse og bekæmpelse af terrorisme og politisk motiveret ekstremistisk vold"* bemærkes det, at terrortruslen mod medlemsstaterne fortsat er høj, og der udtrykkes bekymringer for, at visse ekstremistiske grupper udnytter COVID-19-pandemien til at rekruttere online og offline. Der lægges derfor op til, at medlemslandene styrker forebyggelsesindsatser mod radikalisering og understreger, at der fortsat bør fokuseres på fremmedkrigere og på radikaliserede indsatte i fængsler, når de løslades. Det understreges endvidere, at medlemslandene løbende bør registrere personer, som vurderes at udgøre en terrortrussel eller en trussel for politisk motiveret ekstremistisk vold, i relevante EU-databaser og informationssystemer. I den forbindelse opfordres der til, at medlemslandene opnår en fælles forståelse for farlighedsvurderinger, der ligger til grund for sådanne registreringer.

Drøftelsen forventes at munde ud i en efterfølgende vedtagelse af rådskonklusioner, som forventes at favne et partnerskab, der berører hele retshåndhævelses- og sikkerhedsområdet. Drøftelsen har derfor også forgreninger til en række øvrige emner under RIA-dagsordenen, og således blev etableringen af et europæisk politipartnerskab drøftet på de uformelle videokonferencer for justits- og indenrigsministre den 6.-7. juli 2020. Det tyske formandskab konkluderede her, at der blandt medlemsstaterne var enighed om at styrke politisamarbejdet, og at der skal fokus på finansieringen heraf. Endvidere blev der den 21. oktober 2020 afholdt et virtuelt møde mellem justitsministrene om Europols fremtid. Drøftelsen tog udgangspunkt i et udkast til en rådserklæring om Europols fremtid, der var udarbejdet af det tyske formandskab. Det fremgik heraf bl.a., at Europol skal være partner i det europæiske politipartnerskab, og at Europol fortsat skal understøtte medlemsstaterne med informationsdeling, analyser og ekspertise.

3. Formål og indhold

Formålet med drøftelsen er at etablere et strategisk set-up, hvor man kan sikre et mere effektivt samarbejde medlemsstaterne imellem og herved

højne sikkerheden. Der er på mødet lagt op til en drøftelse af udkastet til rådskonklusionerne.

4. Europa-Parlamentets udtalelser
Europa-Parlamentet skal ikke høres.

5. Nærhedsprincippet
Spørgsmålet om nærhedsprincippet er ikke relevant.

6. Gældende dansk ret
Sagen giver ikke anledning til at redegøre for gældende dansk ret.

7. Konsekvenser
Lovgivningsmæssige konsekvenser
Sagen medfører ikke i sig selv lovgivningsmæssige konsekvenser.

Økonomiske konsekvenser
Sagen medfører ikke i sig selv økonomiske konsekvenser.

Andre konsekvenser og beskyttelsesniveauet
Sagen giver ikke anledning til at fremhæve andre konsekvenser.

8. Høring
Der er ikke foretaget høring vedrørende sagen.

9. Generelle forventninger til andre landes holdninger
Der er generelt opbakning til rådskonklusionerne blandt medlemsstaterne.

10. Regeringens generelle holdning
Danmark deler målsætningen om at sikre bedst mulig beskyttelse af EU's interne sikkerhed. Man kan fra dansk side derfor overordnet støtte udkastet.

I udkastet til rådskonklusionerne er der bl.a. lagt op til, at der skal være et tæt samarbejde med Europol. Danmark er som følge af retsforbeholdet ikke en del af Europol, men Danmark har en samarbejdsaftale med Europol om operativt og strategisk samarbejde.

Danmark støtter indsatser relateret til forebyggelse og bekæmpelse terrorisme og politisk motiveret ekstremistisk vold. Danmark støtter således initiativet om en styrket informationsudveksling mellem medlemsstaternes myndigheder, herunder at personer, der udgør en terrortrussel eller en trussel

for politisk motiveret ekstremistisk vold, registreres i relevante EU-databaser og informationssystemer.

11. Tidligere forelæggelser for Folketingets Europaudvalg

Sagen har tidligere været forelagt for Folketingets Europaudvalg forud for de uformelle videokonferencer mellem justits- og indenrigsministre den 8.-9. oktober 2020. Her var det dog andre fokuspunkter om et europæisk politipartnerskab, der blev drøftet, og ikke de nye fokuspunkter, der fremgår af udkastet til rådskonklusionerne.