JUSTITSMINISTERIET

Dato: 28. november 2018
Kontor: Forebyggelseskontoret
Sagsbeh: Nathalie Bidstrup Nielsen
Sagsnr.: 2018-5000-0079
Dok.: 930122

Bilag I til dagsordenspunkt 1: Forslag til Europa-Parlamentets og Rådets forordning om forebyggelse af udbredelsen af terrorrelateret indhold på nettet i samlenotat vedrørende de sager inden for Justitsministeriets ansvarsområde, der forventes behandlet på rådsmødet (retlige og indre anliggender) og mødet i Det Blandede Udvalg den 6. – 7. december 2018

Som det fremgår af samlenotatet, har Justitsministeriet sendt forordningsforslaget i høring til en række relevante interessenter. Dansk Erhverv, Dansk Industri, Institut for Menneskerettigheder, IT-Politisk Forening og Teleindustrien har afgivet høringssvar med bemærkninger til forslaget.

Dansk Erhverv

Dansk Erhverv (DE) er 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 omfatter potentielt 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.

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

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

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 kan henvise 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 Menneskerettigheders høringssvar

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. Såfremt 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 EMRK 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

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. IFP 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 funktio-

naliteten 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

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. Teleindustriens finder, at en sådan vurdering og beslutning alene bør foretages af domstolene.