EUROPA-
KOMMISSIONEN

Bruxelles, den 12.9.2018
SWD(2018) 409 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUME AF KONSEKVENSANALYSEN

Ledsagedokument til

Forslag til Europa-Parlamentets og Rådets forordning

om forebyggelse af udbredelsen af terrorrelateret onlineindhold

{COM(2018) 640 final} - {SEC(2018) 397 final} - {SWD(2018) 408 final}

Resumé

Konsekvensanalyse om forebyggelse af udbredelsen af terrorrelateret onlineindhold

A. Behov for handling

Hvorfor? Hvad er problemstillingen?

Udbredelsen af terrorrelateret onlineindhold er fortsat et stort og påtrængende samfundsmæssigt og politisk problem. Til trods for en række ikkelovgivningsmæssige foranstaltninger bliver hostingtjenesteydelser stadig brugt til udbredelse af terrorindhold.

Hvilke resultater forventes der af initiativet?

Dette initiativ stiler mod at skabe større tillid til onlinemiljøet i det digitale indre marked ved at begrænse adgangen til terrorindhold på nettet, idet der sørges for et højt sikkerhedsniveau for EU's borgere. Det stiler særligt mod at øge effektiviteten af foranstaltninger til sporing og fjernelse af terrorindhold, og mod at øge hostingtjenesteydernes gennemsigtighed og ansvarlighed. Foranstaltningerne stiler ligeledes mod at forbedre de relevante myndigheders evne til at gribe ind over for terrorindhold på nettet, beskytte mod risikoen for fejlagtig fjernelse af lovligt indhold og sørge for passende beskyttelse af grundlæggende rettigheder.

Hvad er merværdien ved at handle på EU-plan?

De fleste onlineplatforme opererer på tværs af grænser og gør indhold tilgængeligt, uanset hvor brugerne eller indholdsleverandørerne befinder sig. Medlemsstaterne har lovgivet med hensyn til fjernelse af ulovligt indhold på nettet, men behovet for at sikre den offentlige sikkerhed på nationalt niveau skal afvejes i forhold til den grundlæggende ret til udbydelse af tjenesteydelser og etableringsfriheden i henhold til det indre markeds regler.

Der er forskelle på de nationale regler, og de risikerer at blive større, hvilket vil bringe en effektiv udøvelse af etableringsfriheden og retten til udbydelse af tjenesteydelser i EU i fare, alt imens det vil begrænse en effektiv bekæmpelse af terrorrelateret onlineindhold, ligesom det vil føre til øgede overholdelsesomkostninger for virksomhederne.

Medlemsstaternes egne tiltag kan ikke på effektiv vis tackle udfordringen med at begrænse ulovligt indhold på nettet, i betragtning af de berørte tjenesters natur og den voksende fragmentering af det indre marked.

B. Løsninger

Hvilke lovgivningsmæssige og ikkelovgivningsmæssige løsninger er overvejet? Foretrækkes en bestemt løsning frem for andre? Hvorfor?

I konsekvensanalysen blev der ud over basisscenariet vurderet tre løsninger, som afspejler en lignende interventionslogik med forskellige grader af intensitet hvad angår effektivitet og virkning på de grundlæggende rettigheder. Byggestenene for de tre løsninger omfatter:

Bestemmelser om **harmonisering af procedurer for fjernelse eller deaktivering af adgangen til terrorindhold** som følge af et påbud om fjernelse udstedt af en national myndighed. For at fremme procedurerne omfatter harmoniseringen endvidere en **fælles definition af terrorrelateret onlineindhold** (forskellige definitioner overvejes under de tre løsninger) såvel som en præcisering vedrørende den ret til retslige prøvelse, som hostingtjenesteydere og indholdsleverandører har i forbindelse med påbud om fjernelse (fælles for alle løsninger).

Bestemmelser, som skal sikre **gennemsigtige processer og rapportering** til myndigheder og til Kommissionen (ligheder med de andre løsninger) vil øge ansvarligheden og tilliden til indholdshåndteringsprocessen og vil støtte de politiske beslutningstagere og nationale myndigheder i deres bekæmpelse af terrorindhold, ligesom det vil hjælpe brugerne med bedre at forstå, hvordan hostingtjenesteydere anvender deres politik om forvaltning af indhold.

Samarbejde mellem nationale myndigheder og Europol (med forskellig intensitet alt efter løsning) vil forbedre evnen til at gøre en fælles indsats for at bekæmpe terrorindhold, forebygge dobbeltarbejde og reducere

kompleksiteten og omkostningerne for hostingtjenesteyderne i deres interaktion med nationale myndigheder, når de udbyder tjenester på tværs af grænserne.

Desuden sikrer bestemmelser, at hostingtjenesteyderne, i de tilfælde, hvor virksomheder eksponeres for terrorindhold, iværksætter **passende og forholdsmæssige foranstaltninger til proaktiv sporing af terrorindhold** (forskellige krav alt efter løsning).

Sikkerhedsforanstaltninger (fælles for alle løsninger) og bestemmelser, som skal sikre, at de trufne foranstaltninger til sporing og fjernelse af terrorindhold ikke fører til fejlagtig fjernelse af lovligt indhold, og at de grundlæggende rettigheder overholdes.

Bestemmelser, som **sikrer, at foranstaltningerne kan håndhæves** (fælles for alle løsninger), herunder udpegelse af retlige repræsentanter for ikke-EU-virksomheder, etablering af kontaktpunkter og sikring af, at medlemsstaterne har et sammenhængende sanktionssystem på plads.

Rapporten indeholder en kombination af de foranstaltninger, der er vurderet som værende de mest effektive til håndtering af terrorindhold på nettet. Den indeholder ligeledes en evaluering af fordelene ved de forskellige byggesten med hensyn til effektivitet.

Konsekvensanalysen konkluderer, at inkluderende foranstaltninger såsom en omfattende definition af terrorindhold, krav om fjernelse af indhold, der efter et påbud om fjernelse skal fjernes inden for en time, krav om vurdering af indberetninger fra både Europol og medlemsstaterne såvel som krav om, at hostingtjenesteydere eksponeret for terrorindhold skal træffe proaktive foranstaltninger for at spore nyt terrorindhold og forebygge genupload af kendt materiale, samt en solid række sikkerhedsforanstaltninger mod fejlagtig fjernelse af lovligt indhold og gennemsigtighedsforpligtelser vil være mere effektive, når det drejer sig om at nå de politiske målsætninger.

Hvem støtter hvilken løsning?

Hostingtjenesteyderne støtter generelt basisscenariet. De mener, at den fulde effekt af ikkelovgivningsmæssige foranstaltninger bør evalueres først. Hvis der vedtages en retsakt, vil de støtte en målrettet indsats inden for specifikke områder af særlig værdi for offentligheden.

Medlemsstaterne anerkender behovet for yderligere støtteforanstaltninger (f.eks. fortsat udvikling af basisscenariet) og støtter et indgreb, som er målrettet terrorindhold. Medlemsstaterne fremhæver især nødvendigheden af en fælles definition af terrorindhold, krav om handling efter indberetning, proaktive foranstaltninger såvel som gennemsigtighed og foranstaltninger, som gør det lettere at tilgå fjernet indhold til retshåndhævelsesformål. Det Europæiske Råd har opfordret Kommissionen til at forelægge et lovgivningsforslag, der skal forbedre påvisning og fjernelse af indhold, som tilskynder til had og til at begå terrorhandlinger.

Civilsamfundet, som repræsenterer de digitale rettigheder og den akademiske verden, støtter udvikling af basisscenariet. De råder til forsigtighed, når det handler om visse elementer, herunder reguleringsmulighederne, navnlig for så vidt angår proaktive foranstaltninger og virkningerne på grundlæggende rettigheder. Disse betænkeligheder bliver delt af enkeltpersoner i deres svar på den offentlige høring. Et repræsentativt udsnit af borgere, der har svaret på en særlig Eurobarometerundersøgelse, støtter yderligere foranstaltninger på EU-niveau til bekæmpelse af ulovligt indhold på nettet.

C. Omkostninger og fordele ved den foretrukne løsning

I konsekvensanalysen oplistes der for hver løsning omkostninger og fordele ved foranstaltningerne. Analysen konkluderer, at løsning 3 er den mest effektive. Den politiske løsning vil bidrage betydeligt til at nå de politiske målsætninger og give de største fordele i forhold til problemets omfang. Om end den tredje løsning forventes at få de største økonomiske konsekvenser med hensyn til forventede omkostninger og den yderligere administrative byrde, vil den også medføre de største fordele.

D. Opfølgning

Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?

Der vil blive fastlagt et detaljeret program for overvågning af forordningens output, resultater og virkninger, der

kan ligge til grund for en evaluering. Overvågningen vil primært være baseret på de oplysninger, som medlemsstaterne har indhentet hos de kompetente myndigheder i forbindelse med deres opgaver, suppleret med offentligt tilgængelige gennemsigtighedsrapporter. Andre oplysninger om især proaktive foranstaltninger vil blive stillet til rådighed af hostingtjenesteyderne som del af deres rapporteringsforpligtelser. Denne overvågning vil under alle løsninger blive suppleret med forskning med henblik på bedre at forstå udbredelsen af ulovligt indhold på nettet, ligesom den teknologiske udvikling vil blive fulgt med hensyn til automatiserede værktøjer til fjernelse af ulovligt indhold.