Europeiska unionens råd

Bryssel den 14 september 2018
(OR. en)

12129/18

Interinstitutionellt ärende:
2018/0331(COD)

CT 144
ENFOPOL 450
COTER 114
JAI 881
CYBER 193
TELECOM 288
FREMP 142
AUDIO 64
DROIPEN 127
COHOM 107
CODEC 1468

FÖRSLAG

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
inkom den:	14 september 2018
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2018) 640 final
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om förhindrande av spridning av terrorisminnehåll online *Ett bidrag från Europeiska kommissionen till toppmötet i Salzburg den 19–20 september 2018*

För delegationerna bifogas dokument – COM(2018) 640 final.

Bilaga: COM(2018) 640 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om förhindrande av spridning av terrorisminnehåll online

Ett bidrag från Europeiska kommissionen till toppmötet i Salzburg den 19–20 september 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

1.1. Motiv och syfte med förslaget

Tack vare internets stora utbredning är det möjligt för användarna att kommunicera, arbeta och knyta kontakter, liksom att skapa, få tillgång till samt dela information och innehåll med hundratals miljoner personer runtom i världen. Internetplattformar har en avsevärd positiv inverkan på användarnas ekonomiska och sociala välmående såväl inom unionen som utanför. Möjligheten att nå en så stor publik till minimala kostnader lockar dock också brottslingar som vill missbruka internet för olagliga ändamål. De senaste terroristattackerna på EU:s mark har visat hur terrorister missbrukar internet för att lära upp och rekrytera anhängare, förbereda och underlätta terroristverksamhet, förhärliga sina grymheter samt uppmana andra att följa deras exempel och skapa rädsla bland allmänheten.

Terrorisminnehåll som delas online för sådana ändamål sprids via värdtjänstleverantörer som gör det möjligt att ladda upp innehåll från tredje part. Det har visat sig att terrorisminnehåll online kraftigt har bidragit till att radikalisera så kallade ensamvargar och inspirera dem till flera terroristattacker på senare tid i Europa. Sådant innehåll inverkar negativt på enskilda individer och samhället som helhet, men minskar också användarnas förtroende för internet och påverkar de berörda företagens affärsmodeller och anseende. Terrorister har inte bara missbrukat stora sociala medieplattformar, utan i allt större utsträckning även mindre leverantörer som erbjuder olika typer av internationella värdtjänster. Detta missbruk av internet framhäver internetplattformarnas särskilda samhällsansvar för att skydda sina användare från att utsättas för terrorisminnehåll och de allvarliga säkerhetsrisker som detta innehåll innebär för samhället i stort.

Värdtjänstleverantörer har på uppmaning av offentliga myndigheter infört vissa åtgärder för att motverka terrorisminnehåll på sina tjänster. Framsteg har gjorts genom frivilliga system och partnerskap, bland annat EU:s internetforum som lanserades i december 2015 inom ramen för den europeiska säkerhetsagendan. EU:s internetforum har främjat medlemsstaternas och värdtjänstleverantörernas frivilliga samarbete och åtgärder för att minska tillgången till terrorisminnehåll online och ge civilsamhället bättre möjligheter att öka mängden effektiva, alternativa budskap på nätet. Dessa insatser har bidragit till ett ökat samarbete genom att förbättra företagens svar på anmälningar från nationella myndigheter och Europols enhet för anmälan av innehåll på internet, lett till att det införts frivilliga proaktiva åtgärder för att förbättra automatisk upptäckt av terrorisminnehåll samt uppmuntrat ett ökat samarbete inom branschen – bland annat genom utvecklingen av ”databasen över hasher” för att förhindra att känt terrorisminnehåll laddas upp på nytt på anslutna plattformar – och mer transparenta insatser. Samarbetet inom ramen för EU:s internetforum bör fortsätta framöver, men de frivilliga arrangemangen har också visat sig ha begränsningar. För det första deltar inte alla berörda värdtjänstleverantörer i forumet, och för det andra är värdtjänstleverantörernas framsteg på det hela taget varken tillräckligt omfattande eller snabba för att verkligen avhjälpa detta problem.

Med tanke på dessa begränsningar finns det ett klart behov av ytterligare åtgärder från Europeiska unionen mot terrorisminnehåll online. Den 1 mars 2018 antog kommissionen en rekommendation om åtgärder för att effektivt bekämpa olagligt innehåll online, som byggde

på kommissionens meddelande från september[1] samt arbetet inom ramen för EU:s internetforum. I rekommendationen ingår ett särskilt kapitel om åtgärder för att effektivt bromsa upp uppladdning och delning av terroristpropaganda på nätet, såsom förbättringar av anmälningsförfarandet, en tidsfrist på en timme för att svara på anmälningar, mer proaktiv upptäckt, effektivt avlägsnande och tillräckliga skyddsåtgärder för att korrekt bedöma terrorisminnehåll[2].

EU:s medlemsstater har också lyft fram behovet av kraftigare insatser mot terrorisminnehåll online, och några av dem har stiftat lagar om detta eller uttryckt planer på att göra det. Efter en rad terroristattacker i EU och mot bakgrund av att terrorisminnehåll fortfarande är lättillgängligt online, uppmanade Europeiska rådet vid sitt möte den 22–23 juni 2017 sektorn att ”utveckla nya tekniker och verktyg i syfte att förbättra den automatiska upptäckten av och raderingen av innehåll som uppviglar till terroristdåd. Detta bör vid behov kompletteras genom relevanta lagstiftningsåtgärder på EU-nivå”. Europeiska rådet välkomnade vid sitt möte den 28 juni 2018 ”kommissionens avsikt att lägga fram ett lagstiftningsförslag i syfte att förbättra upptäckten och raderingen av innehåll som framkallar hat och uppviglar till terroristdåd”. Dessutom uppmanade Europaparlamentet, i sin resolution om onlineplattformar och den digitala inre marknaden den 15 juni 2017, de berörda plattformarna ”att vidta kraftigare åtgärder mot olagligt och skadligt innehåll” och uppmanade kommissionen att lägga fram förslag för att ta itu med dessa problem.

För att komma till rätta med dessa utmaningar och tillmötesgå medlemsstaternas och Europaparlamentets uppmaningar är avsikten med detta kommissionsförslag att fastställa en tydlig och harmoniserad rättslig ram för att förhindra att värdtjänster missbrukas för spridning av terrorisminnehåll online, i syfte att garantera att den digitala inre marknaden fungerar smidigt och samtidigt säkerställa förtroende och säkerhet. Denna förordning syftar till att klargöra värdtjänstleverantörernas ansvar för att vidta alla lämpliga, rimliga och proportionella åtgärder som krävs för att säkerställa deras tjänsters säkerhet samt snabbt och effektivt upptäcka och avlägsna terrorisminnehåll online, med beaktande av den grundläggande vikten av yttrandefrihet och informationsfrihet i ett öppet och demokratiskt samhälle. Genom förordningen införs också ett antal nödvändiga skyddsåtgärder som är avsedda att säkerställa full respekt för grundläggande rättigheter såsom yttrandefrihet och informationsfrihet i ett demokratiskt samhälle samt möjligheter till rättslig prövning som garanteras av rätten till ett effektivt rättsmedel enligt artikel 19 i fördraget om Europeiska unionen (EU-fördraget) och artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna.

Genom att införa minimikrav på aktsamhet för värdtjänstleverantörerna, däribland vissa specifika regler och skyldigheter, samt skyldigheter för medlemsstaterna, är avsikten med förslaget att effektivisera de befintliga åtgärderna för upptäckt, identifiering och avlägsnande av terrorisminnehåll online, utan att inkräkta på grundläggande rättigheter såsom yttrandefrihet och informationsfrihet. En sådan harmoniserad rättslig ram kommer att underlätta tillhandahållandet av onlinetjänster på den digitala inre marknaden, säkerställa lika villkor för alla värdtjänstleverantörer som riktar sina tjänster till Europeiska unionen samt utgöra en stabil rättslig ram för upptäckt och avlägsnande av terrorisminnehåll, med lämpliga skyddsåtgärder för att skydda de grundläggande rättigheterna. I synnerhet kommer transparenskraven att öka förtroendet bland allmänheten, framför allt internetanvändarna, och

[1] Kommissionens meddelande *Hantering av olagligt innehåll online*, COM(2017) 555 final.

[2] Kommissionens rekommendation av den 1 mars 2018 om åtgärder för att effektivt bekämpa olagligt innehåll online, C(2018) 1177 final.

öka ansvarigheten och transparensen i företagens insatser, även med avseende på offentliga myndigheter. I förslaget fastställs också skyldigheter att införa rättsmedel och klagomålsmekanismer för att säkerställa att användarna kan bestrida avlägsnandet av deras innehåll. Medlemsstaternas skyldigheter kommer att bidra till att dessa mål uppnås samt förbättra de berörda myndigheternas förmåga att vidta lämpliga åtgärder mot terrorisminnehåll online och att bekämpa brottslighet. Om värdtjänstleverantörer underlåter att följa förordningen kan medlemsstaterna besluta om påföljder.

1.2. Förenlighet med EU:s befintliga rättsliga ram inom området

Förslaget är förenligt med regelverket om den digitala inre marknaden, i synnerhet direktivet om elektronisk handel. I synnerhet bör inga åtgärder som en värdtjänstleverantör vidtar i enlighet med denna förordning, inte heller proaktiva åtgärder, i sig leda till att tjänsteleverantören förlorar möjligheten till det undantag från ansvarighet som föreskrivs under vissa förutsättningar i artikel 14 i direktivet om elektronisk handel. Om de nationella myndigheterna fattar ett beslut om att föreskriva proportionella och specifika proaktiva åtgärder bör detta i princip inte leda till införandet av en allmän övervakningsskyldighet i den mening som avses i artikel 15.1 i direktiv 2000/31/EG gentemot medlemsstaterna. Med tanke på de särskilt allvarliga risker som är förknippade med spridning av terrorisminnehåll kan beslut som fattas enligt denna förordning dock i undantagsfall avvika från denna princip enligt EU-regelverket. Innan den behöriga myndigheten fattar sådana beslut bör den finna rätt balans mellan hänsyn till allmän säkerhet och de berörda intressena och grundläggande rättigheterna, framför allt yttrandefrihet, informationsfrihet, näringsfrihet samt skydd av personuppgifter och personlig integritet. Värdtjänstleverantörernas aktsamhetskrav bör återspegla och respektera denna balans som uttrycks i direktivet om elektronisk handel.

Förslaget är också konsekvent med och nära anpassat till direktiv (EU) 2017/541 om bekämpande av terrorism, vars syfte är att harmonisera medlemsstaternas lagstiftning om kriminalisering av terroristbrott. Enligt artikel 21 i direktivet om bekämpande av terrorism ska medlemsstaterna vidta åtgärder för att säkerställa snabbt avlägsnande, men kravet är begränsat till internetinnehåll som utgör en offentlig uppmaning och medlemsstaterna kan själva välja åtgärderna. Genom sin förebyggande natur omfattar denna förordning inte enbart material som uppviglar till terrorism utan även rekryterings- och utbildningsmaterial, vilket återspeglar andra brott med anknytning till terroristverksamhet som också omfattas av direktiv (EU) 2017/541. Denna förordning ålägger värdtjänstleverantörer direkta aktsamhetskrav i fråga om att avlägsna terrorisminnehåll och harmoniserar förfarandena för avlägsnandeorder, i syfte att minska tillgången till terrorisminnehåll online.

Förordningen kompletterar de regler som fastställs i det framtida direktivet om audiovisuella medietjänster såtillvida att den omfattar fler personer och mer material. Förordningen omfattar inte bara videodelningsplattformar, utan alla olika typer av värdtjänstleverantörer. Utöver videor omfattas dessutom bilder och text. Föreliggande förordning går därtill längre än direktivet vad gäller materiella bestämmelser, genom att harmonisera reglerna för begäran om att avlägsna terrorisminnehåll samt proaktiva åtgärder.

Den föreslagna förordningen bygger på kommissionens rekommendation[3] om olagligt innehåll från mars 2018. Rekommendationen är fortfarande i kraft, och alla som har en roll att spela när det gäller att minska tillgången till olagligt innehåll – även terrorisminnehåll – bör fortsätta att anpassa sina insatser till de åtgärder som anges i rekommendationen.

[3] Kommissionens rekommendation av den 1 mars 2018 om åtgärder för att effektivt bekämpa olagligt innehåll online, C(2018) 1177 final.

1.3. Sammanfattning av den föreslagna förordningen

Den personkrets som omfattas av förordningen inbegriper värdtjänstleverantörer som erbjuder sina tjänster inom unionen, oavsett verksamhetsställe eller storlek. I den föreslagna lagstiftningen införs ett antal åtgärder för att förhindra missbruk av värdtjänster för spridning av terrorisminnehåll online, i syfte att garantera att den digitala inre marknaden fungerar smidigt och samtidigt säkerställa förtroende och säkerhet. Definitionen av olagligt terrorisminnehåll stämmer överens med definitionen av terroristbrott i direktiv (EU) 2017/541 och omfattar information som används för att uppvigla till och förhärliga terroristbrott, uppmuntra bidrag till och ge instruktioner om utförande av terroristbrott samt främja deltagande i terroristgrupper.

För att säkerställa att olagligt terrorisminnehåll avlägsnas införs genom förordningen en avlägsnandeorder som kan utfärdas som ett administrativt eller rättsligt beslut av en behörig myndighet i en medlemsstat. I sådana fall är värdtjänstleverantören skyldig att avlägsna innehållet eller göra det oåtkomligt inom en timme. I förordningen harmoniseras dessutom minimikraven på anmälningar som medlemsstaternas behöriga myndigheter och unionsorgan (t.ex. Europol) gör till värdtjänstleverantörer för att bedömas mot deras respektive användarvillkor. Slutligen kräver förordningen att värdtjänstleverantörer, när så är lämpligt, vidtar proaktiva åtgärder som står i proportion till risknivån och avlägsnar terrorisminnehåll från sina tjänster, bland annat genom att använda automatiska verktyg för upptäckt.

Åtgärderna för att minska terrorisminnehållet online åtföljs av ett antal viktiga skyddsåtgärder för att säkerställa ett fullständigt skydd av de grundläggande rättigheterna. Som en del av de åtgärder som ska förhindra att innehåll som inte är terrorisminnehåll avlägsnas felaktigt fastställs i förslaget krav på att införa rättsmedel och klagomålsmekanismer för att säkerställa att användarna kan bestrida avlägsnandet av deras innehåll. I förordningen införs dessutom transparenskrav för de åtgärder som värdtjänstleverantörer vidtar mot terrorisminnehåll, vilket säkerställer ansvarighet gentemot användare, medborgare och offentliga myndigheter.

Enligt förordningen är medlemsstaterna skyldiga att säkerställa att deras behöriga myndigheter har den kapacitet som krävs för att ingripa mot terrorisminnehåll online. Utöver detta är medlemsstaterna skyldiga att informera och samarbeta med varandra och kan använda sig av de kanaler som upprättats av Europol för att säkerställa samordning i fråga om avlägsnandeorder och anmälningar. I förordningen föreskrivs också skyldigheter för värdtjänstleverantörerna att rapportera mer i detalj om de åtgärder som vidtas och informera de brottsbekämpande myndigheterna när de upptäcker innehåll som utgör ett hot mot liv eller säkerhet. Slutligen anges en skyldighet för värdtjänstleverantörerna att bevara det innehåll som de avlägsnar, vilket fungerar som ett skydd mot felaktigt avlägsnande och säkerställer att potentiella bevis som behövs för förebyggande, upptäckt, utredning och lagföring av terroristbrott inte går förlorade.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

2.1. Rättslig grund

Den rättsliga grunden är artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), som föreskriver fastställande av åtgärder för att säkerställa att den inre marknaden fungerar.

Artikel 114 är en lämplig rättslig grund för att harmonisera villkoren för värdtjänstleverantörers utbud av gränsöverskridande tjänster på den digitala inre marknaden och för att jämna ut skillnader mellan medlemsstaternas bestämmelser vilka annars skulle

kunna hindra den inre marknadens funktion. På så sätt förebyggs även framtida hinder för ekonomisk verksamhet som uppstår till följd av skillnader i hur nationell lagstiftning utvecklas.

Artikel 114 i EUF-fördraget kan också användas för att införa skyldigheter för tjänsteleverantörer som är etablerade utanför EU:s territorium när deras tjänster påverkar den inre marknaden, eftersom detta är nödvändigt för det eftersträvade målet för den inre marknaden.

2.2. Val av instrument

Artikel 114 i EUF-fördraget ger unionens lagstiftare möjlighet att anta förordningar och direktiv.

Eftersom förslaget avser skyldigheter för tjänsteleverantörer som vanligen erbjuder sina tjänster i fler än en medlemsstat skulle skillnader i tillämpningen av dessa regler hindra leverantörer som är verksamma i flera medlemsstater från att tillhandahålla sina tjänster. En förordning gör det möjligt att föreskriva samma skyldighet på ett enhetligt sätt i hela unionen, är direkt tillämplig, ger tydlighet och större rättssäkerhet samt förhindrar att reglerna införlivas på olika sätt i medlemsstaterna. Av dessa skäl anses en förordning vara den lämpligaste formen för detta instrument.

2.3. Subsidiaritetsprincipen

Med tanke på de berörda problemens gränsöverskridande dimension måste de åtgärder som ingår i förslaget antas på unionsnivå för att målen ska kunna uppnås. Internet är till sin natur gränsöverskridande, och innehåll som hyses i en medlemsstat går normalt sett att komma åt från vilken medlemsstat som helst.

Det har uppstått en splittrad ram med nationella regler som syftar till att bekämpa terrorisminnehåll online och risken är att splittringen ökar. Detta skulle leda till att det blir en börda för företagen att följa olika föreskrifter och skulle skapa såväl olika villkor för företagen som säkerhetskryphål.

EU-åtgärder stärker därför rättssäkerheten och effektiviserar värdtjänstleverantörernas åtgärder mot terrorisminnehåll online. Detta torde göra det möjligt för fler företag att vidta åtgärder – även företag som är etablerade utanför Europeiska unionen – vilket stärker den digitala inre marknadens integritet.

EU-åtgärder är således motiverade, vilket återspeglar Europeiska rådets slutsatser från juni 2018, där kommissionen uppmanas att lägga fram ett lagstiftningsförslag på detta område.

2.4. Proportionalitetsprincipen

I förslaget fastställs regler om att värdtjänstleverantörer bör vidta åtgärder för att snabbt avlägsna terrorisminnehåll från sina tjänster. Centrala inslag begränsar förslaget till endast vad som är nödvändigt för att uppnå de politiska målen.

I förslaget tas hänsyn till värdtjänstleverantörers arbetsbörda och skyddsåtgärder, bland annat skyddet av yttrandefrihet, informationsfrihet och andra grundläggande rättigheter. Entimmesfristen för avlägsnande gäller endast avlägsnandeorder, för vilka de behöriga myndigheterna har fastställt olaglighet i ett beslut som är föremål för rättslig prövning. För anmälningar fastställs en skyldighet att införa åtgärder för att underlätta en snabb bedömning av terrorisminnehåll, dock utan att föreskriva skyldigheter att avlägsna det eller ange absoluta tidsfrister. Det slutliga beslutet förblir ett frivilligt beslut från värdtjänstleverantörens sida. Företagens arbete med att bedöma innehållet underlättas av att de behöriga myndigheterna i

medlemsstaterna och unionsorganen lämnar förklaringar till varför innehållet kan anses vara terrorisminnehåll. Värdtjänstleverantörer ska, när så är lämpligt, vidta proaktiva åtgärder för att skydda sina tjänster mot spridning av terrorisminnehåll. Specifika krav på proaktiva åtgärder gäller endast de värdtjänstleverantörer som är utsatta för terrorisminnehåll, vilket framgår av att de har tagit emot en avlägsnandeorder som vunnit laga kraft, och bör stå i proportion till risknivån och företagets resurser. Bevarandet av det avlägsnade innehållet och relaterade data är begränsat till en tidsperiod som står i proportion till syftet att möjliggöra administrativ eller rättslig prövning och att förebygga, upptäcka, utreda och lagföra terroristbrott.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

3.1. Samråd med berörda parter

Vid utarbetandet av detta lagstiftningsförslag har kommissionen samrått med alla berörda parter för att förstå deras synpunkter och utröna möjliga sätt att gå vidare. Kommissionen genomförde ett öppet offentligt samråd om åtgärder för att bekämpa olagligt innehåll på ett effektivare sätt och fick in 8 961 svar, varav 8 749 kom från privatpersoner, 172 från organisationer, 10 från offentliga förvaltningar och 30 från andra kategorier av svarande. Parallellt gjordes även en Eurobarometerundersökning om olagligt innehåll på nätet med ett slumpmässigt urval på 33 500 EU-invånare. Kommissionen har också rådgjort med medlemsstaternas myndigheter och tjänsteleverantörer under maj och juni 2018 avseende specifika åtgärder för att bekämpa terrorisminnehåll online.

Överlag konstaterade de flesta berörda parter att terrorisminnehåll online är ett allvarligt samhällsproblem som påverkar internetanvändare och värdtjänstleverantörers affärsmodeller. Mer allmänt ansåg 65 % av deltagarna i Eurobarometerundersökningen[4] att internet inte är säkert för användarna, och 90 % av de tillfrågade ansåg att det är viktigt att begränsa spridningen av olagligt innehåll på nätet. Samråd med medlemsstaterna visade att frivilliga arrangemang visserligen ger resultat, men att många ändå anser att det finns ett behov av bindande skyldigheter avseende terrorisminnehåll, en åsikt som återspeglas i Europeiska rådets slutsatser från juni 2018. Värdtjänstleverantörer var överlag positiva till att fortsätta med de frivilliga åtgärderna, men de noterade de potentiella negativa effekterna av den rättsliga splittring som börjat framträda i unionen.

Många berörda parter konstaterade också behovet av att säkerställa att alla regleringsåtgärder för avlägsnande av innehåll, i synnerhet proaktiva åtgärder och strikta tidsramar, uppvägs av skyddsåtgärder för grundläggande rättigheter, framför allt yttrandefriheten. De berörda parterna noterade ett antal nödvändiga åtgärder i fråga om transparens, ansvarighet och behovet av mänsklig granskning vid användning av automatiska verktyg.

3.2. Konsekvensbedömning

Nämnden för lagstiftningskontroll har lämnat ett positivt yttrande om konsekvensbedömningen, med förbehåll, och gett olika förslag på förbättringar[5]. Efter detta yttrande ändrades konsekvensbedömningen för att beakta nämndens huvudsynpunkter och sätta fokus specifikt på terrorisminnehåll, ytterligare poängtera konsekvenserna för den

[4] Eurobarometer 469 om olagligt innehåll online, juni 2018.

[5] Länk till nämndens yttrande på RegDoc.

digitala inre marknadens funktion samt ge en mer ingående analys av inverkan på de grundläggande rättigheterna och funktionen för de skyddsåtgärder som föreslås i alternativen.

Om inga ytterligare åtgärder vidtas förväntas frivilliga åtgärder enligt grundscenariot fortsätta och i någon mån minska terrorisminnehållet online. Det är dock osannolikt att alla värdtjänstleverantörer som utsätts för sådant innehåll vidtar frivilliga åtgärder, och ytterligare rättslig splittring väntas uppstå, vilket skapar tilläggshinder för gränsöverskridande tillhandahållande av tjänster. Tre huvudalternativ övervägdes utöver grundscenariot, med gradvis större effektivitet i fråga om att uppnå de mål som anges i konsekvensbedömningen och det övergripande politiska målet att minska terrorisminnehållet online.

I alla tre alternativen omfattade skyldigheterna alla värdtjänstleverantörer (personkrets) som är etablerade i EU och i tredjeländer, i den mån de erbjuder tjänster i unionen (geografiskt tillämpningsområde). Med tanke på problemets karaktär och behovet av att undvika missbruk av mindre plattformar omfattar inget av alternativen undantag för små och medelstora företag. Alla alternativ skulle kräva att värdtjänstleverantörer fastställer en rättslig företrädare i EU – även företag som är etablerade utanför EU – för att säkerställa verkställigheten för EU-reglerna. I alla alternativ skulle medlemsstaterna utveckla sanktionsmekanismer.

Alla alternativ föreskrev skapandet av ett nytt, harmoniserat system av rättsligt bindande avlägsnandeorder för terrorisminnehåll online som nationella myndigheter utfärdar till värdtjänstleverantörer, och krav på att avlägsna detta innehåll inom en timme. Dessa order skulle inte nödvändigtvis kräva en bedömning från värdtjänstleverantörernas sida, och skulle kunna bli föremål för rättslig prövning.

Skyddsåtgärderna, i synnerhet klagomålsförfaranden och effektiva rättsmedel – däribland rättslig prövning samt andra bestämmelser för att förhindra att innehåll som inte är terrorisminnehåll avlägsnas felaktigt, samtidigt som iakttagande av de grundläggande rättigheterna säkerställs – är desamma i alla tre alternativen. Dessutom innehåller alla alternativ rapporteringsskyldigheter i form av offentlig transparens och rapportering till medlemsstaterna och kommissionen, samt till myndigheter vid misstänkta brott. Därutöver föreskrivs skyldigheter för nationella myndigheter, värdtjänstleverantörer, och i tillämpliga fall Europol, att samarbeta.

De största skillnaderna mellan de tre alternativen rör omfattningen av definitionen av terrorisminnehåll, nivån på harmonisering av anmälningar, omfattningen av proaktiva åtgärder, medlemsstaternas samordningskrav samt kraven på databevarande. I alternativ 1 skulle det materiella tillämpningsområdet begränsas till innehåll som sprids för att direkt uppvigla till terroristdåd, enligt en snäv definition, medan alternativen 2 och 3 har en vidare ansats som även omfattar rekryterings- och utbildningsmaterial. I fråga om proaktiva åtgärder skulle värdtjänstleverantörer som utsätts för terrorisminnehåll enligt alternativ 1 behöva utföra en riskbedömning, medan proaktiva åtgärder för att motverka risken skulle förbli frivilliga. Enligt alternativ 2 skulle värdtjänstleverantörerna vara skyldiga att utarbeta en handlingsplan som kan inbegripa automatiska verktyg för att förhindra att innehåll som redan har avlägsnats laddas upp på nytt. Alternativ 3 inbegriper mer omfattande proaktiva åtgärder som kräver att tjänsteleverantörer som utsätts för terrorisminnehåll också identifierar nytt material. I alla tre alternativ skulle kraven på proaktiva åtgärder stå i proportion till graden av utsatthet för terrorisminnehåll och tjänsteleverantörens ekonomiska kapacitet. I fråga om anmälningar harmoniseras inte tillvägagångssättet vid anmälningar i alternativ 1, medan det i alternativ 2 görs för Europol och i alternativ 3 även för anmälningar från medlemsstaterna. Enligt alternativen 2 och 3 skulle medlemsstaterna vara skyldiga att informera, samordna sig med och samarbeta med varandra, och enligt alternativ 3 skulle de även vara tvungna att

säkerställa att deras behöriga myndigheter har kapacitet att upptäcka och anmäla terrorisminnehåll. Slutligen innehåller alternativ 3 också ett krav på att bevara data som en skyddsåtgärd i händelse av felaktigt avlägsnande och för att underlätta brottsutredningar.

Utöver de rättsliga bestämmelserna planerades att alla alternativ skulle åtföljas av en rad kompletterande åtgärder, i synnerhet för att underlätta samarbetet mellan de nationella myndigheterna och Europol, samt samverkan med värdtjänstleverantörerna, liksom stöd till forskning, utveckling och innovation för utveckling och införande av tekniska lösningar. Ytterligare medvetandehöjande åtgärder och stödinstrument för små och medelstora företag skulle också kunna införas efter det att rättsakten antagits.

I konsekvensbedömningen drogs slutsatsen att en rad åtgärder krävs för att uppnå det politiska målet. Den omfattande definitionen av terrorisminnehåll som fångar upp det mest skadliga materialet är att föredra framför en smal definition av innehåll (alternativ 1). Proaktiva skyldigheter som är begränsade till att förhindra att terrorisminnehåll laddas upp på nytt (alternativ 2) skulle ha mindre inverkan än skyldigheter i samband med upptäckt av nytt terrorisminnehåll (alternativ 3). Bestämmelser om anmälningar bör omfatta anmälningar från både Europol och medlemsstaterna (alternativ 3) och inte vara begränsade till enbart anmälningar från Europol (alternativ 2), eftersom anmälningar från medlemsstaterna är ett viktigt bidrag till de övergripande försöken att minska tillgången till terrorisminnehåll online. Sådana åtgärder skulle behöva genomföras utöver de åtgärder som är gemensamma för alla alternativ, inklusive stabila skyddsåtgärder mot felaktigt avlägsnande av innehåll.

3.3. Grundläggande rättigheter

Terroristernas onlinepropaganda syftar till att uppvigla enskilda personer till att genomföra terroristattacker, bland annat genom att förse dem med detaljerade anvisningar om hur man vållar största möjliga skada. Efter sådana grymma dåd är det vanligt att terrorister lägger ut ytterligare propaganda som förhärligar dessa handlingar och uppmuntrar andra att följa deras exempel. Denna förordning bidrar till att skydda den allmänna säkerheten genom att minska tillgången till terrorisminnehåll som främjar och uppmuntrar kränkningar av de grundläggande rättigheterna.

Förslaget kan potentiellt påverka ett antal grundläggande rättigheter, såsom

(a) innehållsleverantörens rättigheter: rätten till yttrandefrihet, rätten till skydd av personuppgifter, rätten till respekt för privat- och familjeliv, principen om icke-diskriminering och rätten till ett effektivt rättsmedel,

(b) tjänsteleverantörens rättigheter: näringsfriheten, rätten till ett effektivt rättsmedel,

(c) alla medborgares rättigheter: rätten till yttrande- och informationsfrihet.

Med beaktande av gällande regelverk ingår lämpliga och stabila skyddsåtgärder i den föreslagna förordningen för att säkerställa att dessa personers rättigheter skyddas.

I detta sammanhang fastställs i förordningen inledningsvis en definition av begreppet terrorisminnehåll online i enlighet med definitionen av terroristbrott i direktiv (EU) 2017/541. Denna definition gäller för avlägsnandeorder och anmälningar, liksom för proaktiva åtgärder. Definitionen säkerställer att endast olagligt innehåll som motsvarar en unionsomfattande definition av relaterade brott avlägsnas. Dessutom innehåller förordningen allmänna aktsamhetskrav för värdtjänstleverantörer så att de agerar på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt med avseende på innehåll som de lagrar, i synnerhet när de

tillämpar sina egna användarvillkor, i syfte att undvika att innehåll som inte är terrorisminnehåll avlägsnas.

Mer specifikt har förordningen utformats för att säkerställa att de åtgärder som vidtas är proportionella med avseende på de grundläggande rättigheterna. När det gäller avlägsnandeorder motiveras entimmesfristen för avlägsnande av att en behörig myndighet gjort en bedömning av innehållet (inklusive juridiska kontroller vid behov). Dessutom är förordningens bestämmelser om anmälningar begränsade till sådana som sänds av behöriga myndigheter och unionsorgan med förklaringar till varför innehållet kan anses vara terrorisminnehåll. Även om det fortfarande är värdtjänstleverantören som ansvarar för att avlägsna det innehåll som identifieras i en anmälan underlättas beslutet av nämnda bedömning.

För proaktiva åtgärder ligger ansvaret för att identifiera, bedöma och avlägsna innehåll fortfarande hos värdtjänstleverantörerna, som är skyldiga att införa skyddsåtgärder, bland annat mänsklig granskning, för att säkerställa att innehåll inte avlägsnas felaktigt, i synnerhet om ytterligare sammanhang krävs. Utformningen och genomförandet av åtgärderna skulle dessutom omfattas av rapportering till behöriga organ i medlemsstaterna, till skillnad från grundscenariot där de mest berörda företagen inrättar automatiska verktyg utan offentlig tillsyn. Denna skyldighet minskar risken för felaktiga avlägsnanden både för företag som inför nya verktyg och för företag som redan använder dem. Dessutom måste värdtjänstleverantörer tillhandahålla användarvänliga klagomålsmekanismer så att innehållsleverantörer kan bestrida beslutet om att avlägsna deras innehåll samt offentliggöra transparensrapporter för allmänheten.

Slutligen är värdtjänstleverantörer skyldiga att bevara innehåll under sex månader så att de kan återställa det om innehåll och relaterade data trots dessa skyddsåtgärder felaktigt skulle avlägsnas, för att säkerställa effektiviteten i klagomåls- och prövningsförfarandena i syfte att skydda yttrandefriheten och informationsfriheten. Samtidigt bidrar bevarandet också till brottsbekämpning. Värdtjänstleverantörer måste införa tekniska och organisatoriska skyddsåtgärder för att säkerställa att data inte används för andra ändamål.

De föreslagna åtgärderna, i synnerhet de som rör avlägsnandeorder, anmälningar, proaktiva åtgärder och bevarandet av data, torde inte bara skydda internetanvändarna mot terrorisminnehåll, utan även bidra till att skydda medborgarnas rätt till liv genom att minska tillgången till terrorisminnehåll online.

4. BUDGETKONSEKVENSER

Förslaget till förordning påverkar inte unionens budget.

5. ÖVRIGA INSLAG

5.1. Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering

Senast [ett år efter den dag då denna förordning börjar tillämpas] ska kommissionen upprätta ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter. I övervakningsprogrammet ska det anges indikatorer, vilka metoder som kommer att användas för att samla in uppgifter och andra nödvändiga belägg och med vilka intervaller detta ska ske. Det ska anges vilka åtgärder kommissionen och medlemsstaterna ska vidta för att samla

in och analysera uppgifterna och andra belägg för att övervaka framstegen och utvärdera denna förordning.

På grundval av det fastställda övervakningsprogrammet kommer kommissionen, inom två år efter det att denna förordning trätt i kraft, att rapportera om genomförandet av förordningen utifrån de transparensrapporter som företagen offentliggör samt information från medlemsstaterna. Kommissionen kommer att genomföra en utvärdering tidigast fyra år efter det att förordningen trätt i kraft.

På grundval av utvärderingsresultaten, inklusive huruvida vissa brister eller svagheter kvarstår, och med beaktande av den tekniska utvecklingen, kommer kommissionen att bedöma behovet av att utvidga förordningens tillämpningsområde. Vid behov kommer kommissionen att lägga fram förslag till ändring av denna förordning.

Kommissionen kommer att stödja genomförandet, övervakningen och utvärderingen av förordningen genom en expertgrupp inom kommissionen. Gruppen kommer också att underlätta samarbetet mellan värdtjänstleverantörer, brottsbekämpande myndigheter och Europol, främja utbyten och metoder för att upptäcka och avlägsna terrorisminnehåll, bidra med expertis om hur terroristernas arbetssätt online förändras samt ge råd och vägledning när så är lämpligt för att göra det möjligt att genomföra bestämmelserna.

Genomförandet av den föreslagna förordningen skulle kunna underlättas genom ett antal stödåtgärder. Ett exempel är den möjliga utvecklingen av en plattform inom Europol som kan bidra till samordningen av anmälningar och avlägsnandeorder. EU-finansierad forskning om hur terroristernas arbetssätt förändras ökar alla berörda parters förståelse och medvetenhet. Dessutom stöder Horisont 2020 forskning i syfte att utveckla ny teknik, bland annat automatiserat förhindrande av uppladdning av terrorisminnehåll. Vidare kommer kommissionen att fortsätta att analysera hur man kan stödja behöriga myndigheter och värdtjänstleverantörer i genomförandet av denna förordning genom EU:s finansieringsinstrument.

5.2. Ingående redogörelse för de specifika bestämmelserna i förslaget

I artikel 1 fastställs syftet, och det anges att förordningen innehåller regler för att förhindra missbruk av värdtjänster för spridning av terrorisminnehåll online, inklusive aktsamhetskrav för värdtjänstleverantörer och åtgärder som medlemsstaterna ska vidta. I artikeln fastställs även det geografiska tillämpningsområdet, som omfattar värdtjänstleverantörer som erbjuder tjänster i unionen, oberoende av deras verksamhetsställe.

Artikel 2 innehåller definitioner av de termer som används i förslaget. Där fastställs också en definition av terrorisminnehåll i förebyggande syfte med utgångspunkt i direktivet om bekämpande av terrorism för att fånga upp material och information som uppviglar till, uppmuntrar eller förespråkar utförande av eller bidrag till terroristbrott, ger instruktioner om sådana brott eller främjar deltagande i en terroristgrupps verksamhet.

I artikel 3 anges att värdtjänstleverantörer bör tillämpa aktsamhetskrav när de vidtar åtgärder i enlighet med denna förordning och i synnerhet ta vederbörlig hänsyn till de berörda grundläggande rättigheterna. Enligt artikeln bör lämpliga bestämmelser införas i värdtjänstleverantörernas användarvillkor och det bör säkerställas att dessa tillämpas.

Enligt artikel 4 ska medlemsstaterna ge de behöriga myndigheterna befogenhet att utfärda avlägsnandeorder, och det fastställs krav på att värdtjänstleverantörer avlägsnar innehåll inom en timme efter mottagandet av avlägsnandeordern. Där fastställs också vilken information avlägsnandeordern minst bör innehålla och hur värdtjänstleverantörerna kan ge återkoppling till den utfärdande myndigheten och informera denna om att det inte är möjligt att följa ordern eller att ytterligare klargöranden krävs. Det krävs också att den utfärdande myndigheten informerar den myndighet som utövar tillsyn över proaktiva åtgärder i den medlemsstat som har jurisdiktion över värdtjänstleverantören.

I artikel 5 fastställs krav på att värdtjänstleverantörer inför åtgärder för att snabbt bedöma det innehåll som anmälts av antingen en behörig myndighet i en medlemsstat eller ett unionsorgan, dock utan att kräva att det anmälda innehållet avlägsnas eller fastställa specifika tidsfrister för åtgärder. Där fastställs också vilken information anmälningar minst bör innehålla och hur värdtjänstleverantörerna kan ge återkoppling till den utfärdande myndigheten och begära klargöranden av den myndighet som anmälde innehållet.

Enligt artikel 6 måste värdtjänstleverantörer vidta effektiva och proportionella proaktiva åtgärder när så är lämpligt. Där fastställs ett förfarande som säkerställer att vissa värdtjänstleverantörer (dvs. de som har mottagit en avlägsnandeorder som vunnit laga kraft) vidtar ytterligare proaktiva åtgärder när det är nödvändigt för att minska riskerna och i enlighet med utsattheten för terrorisminnehåll på deras tjänster. Värdtjänstleverantören bör samarbeta med den behöriga myndigheten när det gäller de nödvändiga åtgärder som krävs, och om ingen överenskommelse nås kan myndigheten ålägga tjänsteleverantören att vidta åtgärder. I artikeln fastställs även ett förfarande för prövning av myndighetens beslut.

Enligt artikel 7 måste värdtjänstleverantörer bevara det avlägsnade innehållet och relaterade data i sex månader för prövningsförfaranden och utredningsändamål. Denna period kan förlängas för att göra det möjligt att slutföra prövningen. Enligt artikeln måste tjänsteleverantörerna också införa skyddsåtgärder för att säkerställa att det innehåll och de relaterade data som bevaras inte är åtkomliga eller behandlas för andra ändamål.

I artikel 8 fastställs en skyldighet för värdtjänstleverantörer att förklara sin strategi avseende terrorisminnehåll och offentliggöra årliga transparensrapporter om de åtgärder som vidtagits i detta avseende.

I artikel 9 föreskrivs särskilda skyddsåtgärder avseende användning och genomförande av proaktiva åtgärder vid användning av automatiska verktyg för att säkerställa att beslut är korrekta och välgrundade.

I artikel 10 krävs att värdtjänstleverantörer inrättar klagomålsmekanismer för avlägsnanden, anmälningar och proaktiva åtgärder samt snabbt granskar varje klagomål.

I artikel 11 fastställs en skyldighet för värdtjänstleverantörer att tillhandahålla information om avlägsnandet till innehållsleverantören, förutom när den behöriga myndigheten av hänsyn till allmän säkerhet kräver att denna information inte lämnas ut.

Enligt artikel 12 måste medlemsstaterna säkerställa att de behöriga myndigheterna har den kapacitet och de resurser som behövs för att fullgöra sina skyldigheter enligt denna förordning.

Enligt artikel 13 måste medlemsstaterna samarbeta med varandra, och med Europol när så är lämpligt, för att undvika dubbelarbete och störning av utredningar. I artikeln föreskrivs också en möjlighet för medlemsstaterna och värdtjänstleverantörerna att använda särskilda verktyg, även Europols verktyg, för att handlägga och ge återkoppling om avlägsnandeorder och anmälningar samt samarbeta om proaktiva åtgärder. Medlemsstaterna måste även ha lämpliga kommunikationskanaler för att säkerställa att information utbyts inom rimlig tid vid genomförandet av denna förordning och genomdrivandet av dess bestämmelser. Enligt artikeln är värdtjänstleverantörer även skyldiga att informera de relevanta myndigheterna när de får kännedom om bevis för terroristbrott i den mening som avses i artikel 3 i direktiv (EU) 2017/541 om bekämpande av terrorism.

I artikel 14 föreskrivs att både värdtjänstleverantörerna och medlemsstaterna bör inrätta kontaktpunkter för att underlätta kommunikationen dem emellan, i synnerhet avseende anmälningar och avlägsnandeorder.

I artikel 15 fastställs medlemsstaternas jurisdiktion när det gäller att övervaka proaktiva åtgärder, fastställa påföljder och övervaka arbetet.

I artikel 16 föreskrivs att värdtjänstleverantörer som inte har något verksamhetsställe i en medlemsstat men som erbjuder tjänster inom unionen måste utse en rättslig företrädare i unionen.

Enligt artikel 17 måste medlemsstaterna utse de myndigheter som ska utfärda avlägsnandeorder, anmäla terrorisminnehåll samt övervaka att proaktiva åtgärder genomförs och att förordningen tillämpas.

I artikel 18 anges att medlemsstaterna bör fastställa regler om påföljder för bristande efterlevnad och det anges kriterier som medlemsstaterna bör beakta när de avgör påföljdernas typ och nivå. Med tanke på den särskilda vikten av att snabbt avlägsna terrorisminnehåll som identifierats i en avlägsnandeorder, bör specifika regler införas om böter för systematiska överträdelser av detta krav.

I artikel 19 fastställs ett snabbare och mer flexibelt förfarande för att genom delegerade akter ändra de tillhandahållna mallarna för avlägsnandeorder och autentiserade inlämningskanaler.

I artikel 20 anges på vilka villkor kommissionen har befogenhet att anta delegerade akter för att föreskriva nödvändiga ändringar av mallarna och tekniska krav för avlägsnandeorder.

Enligt artikel 21 måste medlemsstaterna samla in och rapportera specifik information om tillämpningen av förordningen i syfte att bistå kommissionen vid utövandet av dess uppgifter enligt artikel 23. Kommissionen ska upprätta ett detaljerat program för övervakning av utfall, resultat och effekter av denna förordning.

I artikel 22 fastställs att kommissionen ska rapportera om genomförandet av denna förordning två år efter ikraftträdandet.

I artikel 23 fastställs att kommissionen ska rapportera om utvärderingen av denna förordning tidigast tre år efter ikraftträdandet.

I artikel 24 fastställs att den föreslagna förordningen träder i kraft den tjugonde dagen efter det att den offentliggörs i *Europeiska unionens officiella tidning* och kommer att börja tillämpas sex månader efter ikraftträdandet. Denna tidsram föreslås med beaktande av behovet av att genomföra åtgärder samtidigt som det erkänns att det brådskar att tillämpa reglerna i den föreslagna förordningen fullt ut. Tidsramen på sex månader har fastställts utifrån antagandet att förhandlingarna kommer att genomföras snabbt.

2018/0331 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om förhindrande av spridning av terrorisminnehåll online

Ett bidrag från Europeiska kommissionen till toppmötet i Salzburg den 19–20 september 2018

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[6],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Denna förordning syftar till att säkerställa att den digitala inre marknaden fungerar smidigt i ett öppet och demokratiskt samhälle, genom att förhindra att värdtjänster missbrukas för terrorismändamål. Den digitala inre marknadens funktion bör förbättras genom att öka rättssäkerheten för värdtjänstleverantörer, stärka användarnas förtroende för onlinemiljön och förbättra skyddet för yttrandefriheten och informationsfriheten.

(2) Värdtjänstleverantörer som är aktiva på internet spelar en viktig roll i den digitala ekonomin genom att koppla samman företag och medborgare samt genom att underlätta den offentliga debatten och spridningen och mottagandet av information, åsikter och idéer, vilket i hög grad bidrar till innovation, ekonomisk tillväxt och skapande av arbetstillfällen i unionen. Deras tjänster missbrukas dock i vissa fall av tredje part för att bedriva olaglig verksamhet på nätet. Särskilt oroande är att terroristgrupper och deras anhängare utnyttjar värdtjänsteleverantörer för att sprida terrorisminnehåll online i syfte att få ut sitt budskap, radikalisera och rekrytera samt att främja och styra terroristverksamhet.

(3) Förekomsten av terrorisminnehåll online har allvarliga negativa konsekvenser för användare, medborgare och samhället i stort samt för de tjänsteleverantörer som hyser sådant innehåll online, eftersom det undergräver användarnas förtroende och skadar deras affärsmodeller. Med tanke på onlinetjänsteleverantörernas centrala roll och de

[6] EUT C , , s. .

tekniska resurser och den tekniska kapacitet som förknippas med deras tjänster, har de ett särskilt samhällsansvar att skydda sina tjänster mot terroristmissbruk och bidra till att förhindra att terrorisminnehåll sprids via deras tjänster.

(4) Unionens insatser för att motverka terrorisminnehåll online inleddes 2015 genom en ram för frivilligt samarbete mellan medlemsstaterna och värdtjänstleverantörerna, som nu behöver kompletteras med en tydlig rättslig ram för att ytterligare minska tillgången till terrorisminnehåll online och på lämpligt sätt ta itu med ett snabbt växande problem. Avsikten med denna rättsliga ram är att bygga vidare på frivilliga insatser, som förstärktes genom kommissionens rekommendation (EU) 2018/334[7], och tillmötesgå uppmaningarna från Europaparlamentet att vidta kraftigare åtgärder mot olagligt och skadligt innehåll och från Europeiska rådet att förbättra den automatiska upptäckten och raderingen av innehåll som uppviglar till terroristdåd.

(5) Tillämpningen av denna förordning bör inte påverka tillämpningen av artikel 14 i direktiv 2000/31/EG[8]. I synnerhet bör inga åtgärder som en värdtjänstleverantör vidtar i enlighet med denna förordning, inte heller proaktiva åtgärder, i sig leda till att tjänsteleverantören förlorar möjligheten till det undantag från ansvarighet som föreskrivs i den artikeln. Denna förordning påverkar inte de nationella myndigheternas och domstolarnas befogenheter att fastställa värdtjänstleverantörernas ansvar i specifika fall när villkoren för undantag från ansvarighet i artikel 14 i direktiv 2000/31/EG inte är uppfyllda.

(6) Regler för att förhindra att värdtjänster missbrukas för spridning av terrorisminnehåll online anges i denna förordning i syfte att garantera att den inre marknaden fungerar smidigt, med full respekt för de grundläggande rättigheter som skyddas i unionens rättsordning och i synnerhet de som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna.

(7) Denna förordning bidrar till att skydda den allmänna säkerheten, samtidigt som lämpliga och stabila skyddsåtgärder fastställs för att säkerställa skyddet av de grundläggande rättigheter som berörs. Hit hör rätten till respekt för privatlivet och skydd av personuppgifter, rätten till ett effektivt rättsligt skydd, rätten till yttrandefrihet (inklusive friheten att ta emot och sprida uppgifter), näringsfriheten samt principen om icke-diskriminering. Behöriga myndigheter och värdtjänstleverantörer bör endast vidta åtgärder som är nödvändiga, lämpliga och proportionella i ett demokratiskt samhälle, med beaktande av den särskilda vikt som tillmäts yttrandefriheten och informationsfriheten, som utgör en väsentlig grund för ett pluralistiskt, demokratiskt samhälle och är ett av unionens grundläggande värden. Åtgärder som utgör ingrepp i yttrandefriheten och informationsfriheten bör vara strikt riktade, i den bemärkelsen att de måste tjäna till att förhindra spridning av terrorisminnehåll, men utan att därigenom påverka rätten att lagligen ta emot och sprida uppgifter, med beaktande av värdtjänstleverantörernas centrala roll i att främja offentlig debatt samt delande och mottagande av fakta, åsikter och idéer i enlighet med lagen.

---

7 Kommissionens rekommendation (EU) 2018/334 av den 1 mars 2018 om åtgärder för att effektivt bekämpa olagligt innehåll online (EUT L 63, 6.3.2018, s. 50).

8 Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1).

(8) Rätten till ett effektivt rättsmedel fastställs i artikel 19 i EU-fördraget och artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna. Varje fysisk eller juridisk person har rätt till ett effektivt rättsmedel inför behörig nationell domstol mot alla åtgärder som vidtas enligt denna förordning och som kan inverka negativt på den personens rättigheter. Rätten inbegriper särskilt värdtjänstleverantörernas och innehållsleverantörernas möjlighet att effektivt bestrida avlägsnandeorder inför domstol i den medlemsstat vars myndigheter utfärdade avlägsnandeordern.

(9) För att ge klarhet om de åtgärder som både värdtjänstleverantörer och behöriga myndigheter bör vidta för att förhindra spridning av terrorisminnehåll online, bör denna förordning innehålla en definition av terrorisminnehåll i förebyggande syfte vilken utgår från definitionen av terroristbrott i Europaparlamentets och rådets direktiv (EU) 2017/541[9]. Med tanke på behovet av att motverka den skadligaste terroristpropagandan online bör definitionen omfatta material och information som uppviglar till, uppmuntrar eller förespråkar utförande av eller bidrag till terroristbrott, ger instruktioner om utförande av sådana brott eller främjar deltagande i en terroristgrupps verksamhet. Sådan information inbegriper i synnerhet text, bilder, ljudupptagningar och videor. Vid bedömningen av huruvida innehåll utgör terrorisminnehåll i den mening som avses i denna förordning bör de behöriga myndigheterna och värdtjänstleverantörerna ta hänsyn till sådana faktorer som karaktären hos och formuleringen av uttalandena, i vilket sammanhang de gjordes samt deras potential att få skadliga konsekvenser och därigenom påverka människors säkerhet. Det faktum att materialet producerats av, kan tillskrivas eller sprids på uppdrag av en organisation eller person som är uppförd på EU:s terroristförteckning utgör en viktig faktor i bedömningen. Innehåll som sprids i utbildningssyfte, journalistiskt syfte eller forskningssyfte bör skyddas på lämpligt sätt. Dessutom bör det gå att uttrycka radikala, polemiska eller kontroversiella åsikter i den offentliga debatten om känsliga politiska frågor utan att detta ska anses vara terrorisminnehåll.

(10) För att omfatta de onlinevärdtjänster där terrorisminnehåll sprids, bör denna förordning tillämpas på informationssamhällets tjänster som på begäran av en tjänstemottagare lagrar information som tillhandahållits av denna tjänstemottagare och gör den lagrade informationen tillgänglig för tredje part, oavsett om denna verksamhet är av rent teknisk, automatisk och passiv karaktär. Sådana leverantörer av informationssamhällets tjänster är till exempel sociala medieplattformar, direktuppspelningstjänster, video-, bild- och ljuddelningstjänster, fildelningstjänster och andra molntjänster i den mån som de gör informationen tillgänglig för tredje part samt webbplatser där användarna kan kommentera eller lägga upp recensioner. Förordningen bör också tillämpas på värdtjänstleverantörer som är etablerade utanför unionen men erbjuder tjänster inom unionen, eftersom en betydande andel av de värdtjänstleverantörer som är utsatta för terrorisminnehåll på sina tjänster är etablerade i tredjeländer. Detta bör säkerställa att alla företag som är verksamma på den digitala inre marknaden uppfyller samma krav, oavsett etableringsland. För att fastställa om en tjänsteleverantör erbjuder tjänster i unionen krävs en bedömning av huruvida tjänsteleverantören gör det möjligt för juridiska eller fysiska personer i en eller flera medlemsstater att använda dess tjänster. Enbart det faktum att en tjänsteleverantörs webbplats, e-postadress och andra kontaktuppgifter är tillgängliga i en eller flera

[9] Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017 s. 6).

medlemsstater bör dock inte i sig vara tillräckligt för att denna förordning ska kunna tillämpas.

(11) En betydande anknytning till unionen bör vara relevant för att fastställa tillämpningsområdet för denna förordning. En sådan betydande anknytning till unionen bör anses föreligga om tjänsteleverantören har ett verksamhetsställe i unionen eller, i brist på det, på grundval av att det finns ett betydande antal användare i en eller flera medlemsstater eller att verksamheten riktas till en eller flera medlemsstater. Huruvida verksamheten är riktad till en eller flera medlemsstater kan avgöras på grundval av alla relevanta omständigheter, t.ex. faktorer som användning av ett språk eller en valuta som i allmänhet används i den medlemsstaten, eller möjligheten att beställa varor eller tjänster. Verksamheten kan även anses vara riktad till en medlemsstat om en app finns tillgänglig i den berörda nationella appbutiken, om lokal marknadsföring eller reklam görs på det språk som används i medlemsstaten eller om kundkontakter, t.ex. kundtjänst, sköts på det språk som vanligen används i den medlemsstaten. En betydande anknytning bör också antas föreligga om en tjänsteleverantör riktar sin verksamhet till en eller flera medlemsstater i den mening som avses i artikel 17.1 c i Europaparlamentets och rådets förordning (EU) nr 1215/2012[10]. Däremot kan det inte enbart på grund av att en tjänst tillhandahålls för att efterleva det förbud mot diskriminering som fastställs i Europaparlamentets och rådets förordning (EU) 2018/302[11] anses att verksamheten riktas till ett visst territorium inom unionen.

(12) Värdtjänstleverantörer bör följa vissa aktsamhetskrav för att förhindra att terrorisminnehåll sprids på deras tjänster. Dessa aktsamhetskrav bör inte utgöra en allmän övervakningsskyldighet. Aktsamhetskraven bör omfatta att värdtjänstleverantörer, när de tillämpar denna förordning, agerar på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt med avseende på innehåll som de lagrar, i synnerhet när de tillämpar sina egna användarvillkor, i syfte att undvika att innehåll som inte är terrorisminnehåll avlägsnas. När innehåll avlägsnas eller görs oåtkomligt måste det ske med hänsyn till yttrandefriheten och informationsfriheten.

(13) En harmonisering bör ske av förfarandet för och de skyldigheter som följer av rättsliga beslut som ålägger värdtjänstleverantörer att avlägsna terrorisminnehåll eller göra det oåtkomligt efter en bedömning av de behöriga myndigheterna. Medlemsstaterna bör ha fortsatt frihet att välja de behöriga myndigheterna, så att de kan utse administrativa, brottsbekämpande eller rättsliga myndigheter för denna uppgift. Med tanke på hur snabbt terrorisminnehåll sprids via onlinetjänster åläggs värdtjänstleverantörerna i denna förordning skyldigheter att säkerställa att det terrorisminnehåll som anges i avlägsnandeordern avlägsnas eller görs oåtkomligt inom en timme från mottagandet av avlägsnandeordern. Det är upp till värdtjänstleverantörerna att besluta om de ska avlägsna innehållet i fråga eller göra det oåtkomligt för användarna i unionen.

(14) Den behöriga myndigheten bör översända avlägsnandeordern direkt till mottagaren och kontaktpunkten på ett elektroniskt sätt som gör det möjligt att få en skriftlig

---

10 Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (EUT L 351, 20.12.2012, s. 1).

11 Europaparlamentets och rådets förordning (EU) 2018/302 av den 28 februari 2018 om åtgärder mot omotiverad geoblockering och andra former av diskriminering på grund av kunders nationalitet, bosättningsort eller etableringsort på den inre marknaden och om ändring av förordningarna (EG) nr 2006/2004 och (EU) 2017/2394 samt direktiv 2009/22/EG (EUT L 601, 2.3.2018, s. 1).

uppteckning och som ger förutsättningar för tjänsteleverantören att säkerställa autentisering – även att datum och tidpunkt för sändandet och mottagandet av ordern är korrekt – såsom genom säkrad e-post, säkrade plattformar eller andra säkra kanaler, även sådana som tillhandahålls av tjänsteleverantören, i enlighet med reglerna om skydd av personuppgifter. Detta krav kan särskilt uppfyllas genom användning av en kvalificerad elektronisk tjänst för rekommenderad leverans i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 [12].

(15) Anmälningar från de behöriga myndigheterna eller Europol utgör ett effektivt och snabbt sätt att göra värdtjänstleverantörer medvetna om specifikt innehåll på deras tjänster. Denna mekanism för att uppmärksamma värdtjänstleverantörer på information som kan anses vara terrorisminnehåll, så att de på frivillig basis kan bedöma om innehållet är förenligt med de egna användarvillkoren, bör förbli tillgänglig vid sidan av avlägsnandeorder. Det är viktigt att värdtjänstleverantörer bedömer dessa anmälningar som en prioriterad fråga och ger snabb återkoppling om de åtgärder som vidtagits. Det är fortsättningsvis värdtjänstleverantören som fattar det slutliga beslutet om huruvida innehållet ska avlägsnas eftersom det inte är förenligt med användarvillkoren. Europols mandat som fastställs i förordning (EU) 2016/794[13] påverkas inte av tillämpningen av denna förordning när det gäller anmälningar.

(16) Med tanke på terrorisminnehållets omfattning och den snabbhet som krävs för att effektivt identifiera och avlägsna det, är proportionella proaktiva åtgärder, även användning av automatiska metoder i vissa fall, en avgörande del i bekämpandet av terrorisminnehåll online. I syfte att minska tillgången till terrorisminnehåll på värdtjänstleverantörernas tjänster, bör de bedöma om det är lämpligt att vidta proaktiva åtgärder beroende på riskerna för och graden av utsatthet för terrorisminnehåll, samt inverkan på tredje parters rättigheter och allmänhetens intresse av information. Därför bör värdtjänstleverantörer fastställa vilken lämplig, effektiv och proportionell proaktiv åtgärd som bör vidtas. Detta krav bör inte innebära någon allmän övervakningsskyldighet. I samband med denna bedömning är det ett tecken på en låg nivå av utsatthet för terrorisminnehåll om inga avlägsnandeorder och anmälningar har riktats till värdtjänstleverantören.

(17) När proaktiva åtgärder införs bör värdtjänstleverantörer säkerställa att användarnas rätt till yttrandefrihet och informationsfrihet – inklusive friheten att ta emot och sprida uppgifter – bibehålls. Utöver de krav som fastställs i lagstiftning, även lagstiftningen om skydd av personuppgifter, bör värdtjänstleverantörer agera med vederbörlig omsorg och vidta skyddsåtgärder, framför allt mänsklig tillsyn och kontroll, när så är lämpligt, för att undvika oavsiktliga och felaktiga beslut som leder till att innehåll som inte är terrorisminnehåll avlägsnas. Detta är särskilt relevant när värdtjänstleverantörerna använder automatiska metoder för att upptäcka terrorisminnehåll. Beslut om att använda automatiska metoder, oavsett om de fattats av värdtjänstleverantören själv eller efter en begäran från den behöriga myndigheten,

---

12 Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

13 Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).

bör bedömas med hänsyn till den underliggande teknikens tillförlitlighet och den resulterande inverkan på de grundläggande rättigheterna.

(18) För att säkerställa att de värdtjänstleverantörer som utsätts för terrorisminnehåll vidtar lämpliga åtgärder för att förhindra att deras tjänster missbrukas, bör de behöriga myndigheterna begära att värdtjänstleverantörer som har mottagit en avlägsnandeorder som vunnit laga kraft rapporterar om vilka proaktiva åtgärder som vidtagits. Dessa kan bestå av åtgärder för att förhindra att terrorisminnehåll som avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder eller en anmälan laddas upp på nytt, genom en kontroll mot offentliga eller privata verktyg som omfattar känt terrorisminnehåll. De får också använda tillförlitliga tekniska verktyg för att identifiera nytt terrorisminnehåll, antingen sådana som finns tillgängliga på marknaden eller sådana som värdtjänstleverantören har utvecklat. Tjänsteleverantören bör rapportera om de specifika proaktiva åtgärder som vidtagits för att göra det möjligt för den behöriga myndigheten att bedöma om åtgärderna är effektiva och proportionella och, om automatiska metoder används, huruvida värdtjänstleverantören har de nödvändiga förutsättningarna för mänsklig tillsyn och kontroll. Vid bedömningen av åtgärdernas effektivitet och proportionalitet bör de behöriga myndigheterna beakta relevanta parametrar såsom antalet avlägsnandeorder och anmälningar som utfärdats till leverantören, dess ekonomiska kapacitet och tjänstens inverkan på spridningen av terrorisminnehåll (t.ex. med beaktande av antalet användare i unionen).

(19) Efter begäran bör den behöriga myndigheten inleda en dialog med värdtjänstleverantören om de nödvändiga proaktiva åtgärder som ska vidtas. Vid behov bör den behöriga myndigheten föreskriva antagande av lämpliga, effektiva och proportionella proaktiva åtgärder om den anser att de åtgärder som vidtagits inte är tillräckliga för att hantera riskerna. Ett beslut att föreskriva sådana specifika proaktiva åtgärder bör i princip inte leda till införandet av en allmän övervakningsskyldighet i den mening som avses i artikel 15.1 i direktiv 2000/31/EG. Med tanke på de särskilt allvarliga risker som är förknippade med spridningen av terrorisminnehåll, kan de beslut som fattas av de behöriga myndigheterna på grundval av denna förordning avvika från den metod som fastställs i artikel 15.1 i direktiv 2000/31/EG när det gäller vissa specifika, riktade åtgärder som antas av tvingande hänsyn till allmän säkerhet. Innan den behöriga myndigheten fattar sådana beslut bör den finna rätt balans mellan hänsyn till allmän säkerhet och de berörda grundläggande rättigheterna, framför allt yttrandefriheten, informationsfriheten och näringsfriheten, samt lämna en lämplig motivering.

(20) Värdtjänstleverantörernas skyldighet att bevara avlägsnat innehåll och relaterade data bör fastställas för specifika ändamål och tidsbegränsas till den period som är nödvändig. Det finns ett behov av att utvidga bevarandekravet till relaterade data i den mån sådana data annars skulle gå förlorade till följd av att det berörda innehållet avlägsnades. Relaterade data kan omfatta data såsom ”abonnentdata”, t.ex. uppgifter om innehållsleverantörens identitet, och ”åtkomstdata”, t.ex. uppgifter om datum och tidpunkt för innehållsleverantörens användning av eller inloggning till och utloggning från tjänsten, tillsammans med den ip-adress som internetleverantören har tilldelat innehållsleverantören.

(21) Skyldigheten att bevara innehållet för administrativa eller rättsliga prövningsförfaranden är nödvändig och motiverad för att säkerställa effektiv prövning för den innehållsleverantör vars innehåll har avlägsnats eller gjorts oåtkomligt samt för att säkerställa att innehållet kan återställas i samma skick beroende på resultatet av prövningsförfarandet. Skyldigheten att bevara innehåll för utrednings- och

lagföringsändamål är motiverad och nödvändig med tanke på det värde som detta material kan tillföra för att störa eller förhindra terroristverksamhet. Om företag avlägsnar material eller gör det oåtkomligt, i synnerhet genom egna proaktiva åtgärder, och inte informerar den berörda myndigheten eftersom de bedömer att det inte omfattas av artikel 13.4 i denna förordning, kan de brottsbekämpande myndigheterna vara omedvetna om att innehållet existerar. Därför är det också motiverat att bevara innehåll för att förebygga, upptäcka, utreda och lagföra terroristbrott. För dessa ändamål är kravet på att bevara data begränsat till data som sannolikt har samband med terroristbrott och därmed kan bidra till att lagföra terroristbrott eller förhindra allvarliga risker för den allmänna säkerheten.

(22) För att säkerställa proportionalitet bör perioden för bevarande vara begränsad till sex månader så att innehållsleverantörerna får tillräckligt med tid för att inleda prövningsförfarandet och så att brottsbekämpande myndigheter ska kunna få åtkomst till relevanta data för utredning och lagföring av terroristbrott. Denna period kan dock förlängas med den tid som är nödvändig om prövningsförfaranden inleds men inte avslutas inom sexmånadersperioden, på begäran av den myndighet som genomför prövningen. Denna period bör vara tillräcklig för att de brottsbekämpande myndigheterna ska kunna bevara bevis som är nödvändiga för utredningar, samtidigt som balansen i förhållande till de berörda grundläggande rättigheterna säkerställs.

(23) Denna förordning påverkar inte de procedurgarantier och processuella utredningsåtgärder som rör åtkomst till innehåll och relaterade data som bevarats för att utreda och lagföra terroristbrott, vilka fastställs i medlemsstaternas nationella lagstiftning och unionslagstiftningen.

(24) Transparens i värdtjänstleverantörernas strategier för terrorisminnehåll är avgörande för att öka deras ansvarighet gentemot användarna och stärka medborgarnas förtroende för den digitala inre marknaden. Värdtjänstleverantörer bör offentliggöra årliga transparensrapporter som innehåller meningsfull information om åtgärder som vidtagits för att upptäcka, identifiera och avlägsna terrorisminnehåll.

(25) Klagomålsförfaranden utgör en nödvändig skyddsåtgärd mot felaktigt avlägsnande av innehåll som är skyddat genom yttrandefriheten och informationsfriheten. Värdtjänstleverantörer bör därför upprätta användarvänliga klagomålsmekanismer och säkerställa att klagomål hanteras snabbt och med full transparens gentemot innehållsleverantören. Kravet på att värdtjänstleverantören ska återställa innehållet om det har avlägsnats felaktigt påverkar inte värdtjänstleverantörernas möjlighet att genomdriva sina egna användarvillkor på andra grunder.

(26) För ett effektivt rättsligt skydd enligt artikel 19 i EU-fördraget och artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna krävs att personer ska kunna utröna av vilka orsaker det innehåll de laddat upp har avlägsnats eller gjorts oåtkomligt. För detta ändamål bör värdtjänstleverantören tillhandahålla innehållsleverantören meningsfull information som gör det möjligt för innehållsleverantören att bestrida beslutet. Detta kräver dock inte nödvändigtvis en underrättelse till innehållsleverantören. Beroende på omständigheterna kan värdtjänstleverantörer ersätta innehåll som anses vara terrorisminnehåll med ett meddelande om att det har avlägsnats eller gjorts oåtkomligt i enlighet med denna förordning. Ytterligare information om orsakerna och innehållsleverantörens möjligheter att bestrida beslutet bör ges på begäran. Om de behöriga myndigheterna beslutar att det av hänsyn till allmän säkerhet, t.ex. inom ramen för en utredning, är olämpligt eller kontraproduktivt att direkt underrätta innehållsleverantören om att

innehåll har avlägsnats eller gjorts oåtkomligt, bör de informera värdtjänstleverantören.

(27) För att undvika dubbelarbete och möjlig störning av utredningar, bör de behöriga myndigheterna informera, samordna sig med och samarbeta med varandra och Europol, när så är lämpligt, när de utfärdar avlägsnandeorder eller anmäler innehåll till värdtjänstleverantörer. Vid genomförandet av bestämmelserna i denna förordning kan Europol tillhandahålla stöd i enlighet med dess nuvarande mandat och befintliga rättsliga ram.

(28) I syfte att säkerställa ett effektivt och tillräckligt enhetligt genomförande av proaktiva åtgärder bör de behöriga myndigheterna i medlemsstaterna samarbeta med varandra i fråga om de diskussioner de har med värdtjänstleverantörerna avseende identifiering, genomförande och bedömning av specifika proaktiva åtgärder. Ett sådant samarbete behövs också i samband med antagandet av regler om påföljder, samt genomförandet och verkställandet av påföljderna.

(29) Det är viktigt att den behöriga myndigheten i den medlemsstat som är ansvarig för att utdöma påföljder är fullständigt informerad om utfärdandet av avlägsnandeorder och anmälningar samt efterföljande utbyten mellan värdtjänstleverantören och den relevanta behöriga myndigheten. För detta ändamål bör medlemsstaterna säkerställa lämpliga kommunikationskanaler och mekanismer som gör det möjligt att dela den relevanta informationen i rätt tid.

(30) För att underlätta ett snabbt utbyte mellan behöriga myndigheter och värdtjänstleverantörer, och för att undvika dubbelarbete, får medlemsstaterna använda sig av de verktyg som utvecklats av Europol, såsom den befintliga *Internet Referral Management application* (IRMa) eller efterföljare till detta verktyg.

(31) Med tanke på de särskilt allvarliga konsekvenserna av visst terrorisminnehåll, bör värdtjänstleverantörer omgående informera myndigheterna i den berörda medlemsstaten eller de behöriga myndigheterna där de är etablerade eller har en rättslig företrädare om förekomsten av bevis för terroristbrott som de får kännedom om. För att säkerställa proportionalitet är denna skyldighet begränsad till terroristbrott enligt definitionen i artikel 3.1 i direktiv (EU) 2017/541. Informationsskyldigheten innebär inte att värdtjänstleverantörer är skyldiga att aktivt söka sådana bevis. Den berörda medlemsstaten är den medlemsstat som har jurisdiktion över utredning och lagföring av terroristbrott enligt direktiv (EU) 2017/541 på grundval av gärningsmannens eller det potentiella brottsoffrets nationalitet eller målplatsen för terroristdådet. I tveksamma fall får värdtjänstleverantörer överföra informationen till Europol som bör följa upp den i enlighet med sitt mandat, t.ex. genom att vidarebefordra den till de relevanta nationella myndigheterna.

(32) De behöriga myndigheterna i medlemsstaterna bör ha rätt att använda sådan information för att vidta utredningsåtgärder som föreskrivs i medlemsstaternas eller unionens lagstiftning, även att utfärda en europeisk utlämnandeorder enligt förordningen om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden[14].

(33) Både värdtjänstleverantörer och medlemsstaterna bör upprätta kontaktpunkter för att underlätta en snabb handläggning av avlägsnandeorder och anmälningar. I motsats till den rättsliga företrädaren tjänar kontaktpunkten operativa syften.

[14] COM(2018) 225 final.

Värdtjänstleverantörens kontaktpunkt bör bestå av någon typ av särskilda medel som möjliggör elektronisk inlämning av avlägsnandeorder och anmälningar och av tekniska resurser och personalresurser som möjliggör snabb handläggning av dem. Värdtjänstleverantörens kontaktpunkt måste inte vara belägen i unionen, och värdtjänstleverantören är fri att utse en befintlig kontaktpunkt, under förutsättning att denna kontaktpunkt klarar av att fullgöra de funktioner som föreskrivs i denna förordning. I syfte att säkerställa att terrorisminnehåll avlägsnas eller görs oåtkomligt inom en timme från mottagandet av en avlägsnandeorder, bör värdtjänstleverantörerna säkerställa att kontaktpunkten kan nås dygnet runt varje dag. Informationen om kontaktpunkten bör inbegripa information om vilket språk kontaktpunkten kan kontaktas på. För att underlätta kommunikationen mellan värdtjänstleverantörerna och de behöriga myndigheterna, uppmuntras värdtjänstleverantörer att tillåta kommunikation på ett av unionens officiella språk som deras användarvillkor finns tillgängliga på.

(34) Då det inte finns något allmänt krav på att tjänsteleverantörer måste säkerställa fysisk närvaro på unionens territorium, finns det ett behov av att säkerställa klarhet om vilken medlemsstats jurisdiktion den värdtjänstleverantör som erbjuder tjänster inom unionen omfattas av. Som en allmän regel omfattas värdtjänstleverantören av jurisdiktionen i den medlemsstat där den har sitt huvudsakliga verksamhetsställe eller där den har utsett en rättslig företrädare. Om en annan medlemsstat utfärdar en avlägsnandeorder bör det dock vara möjligt för dess myndigheter att genomdriva sin order genom att vidta tvångsåtgärder av en icke-bestraffande karaktär, såsom vite. När det gäller en värdtjänstleverantör som inte har något verksamhetsställe i unionen och som inte utser en rättslig företrädare, bör alla medlemsstater ändå kunna utdöma påföljder, under förutsättning att principen *ne bis in idem* följs.

(35) Värdtjänstleverantörer som inte är etablerade i unionen bör skriftligen utse en rättslig företrädare för att säkerställa att skyldigheterna enligt denna förordning efterlevs och verkställs.

(36) Den rättsliga företrädaren bör ha rättslig befogenhet att agera på värdtjänstleverantörens vägnar.

(37) Medlemsstaterna bör utse behöriga myndigheter för tillämpningen av denna förordning. Kravet på att utse behöriga myndigheter förutsätter inte nödvändigtvis att nya myndigheter inrättas, utan de kan vara befintliga organ som ges i uppdrag att sköta de funktioner som anges i denna förordning. Denna förordning kräver att det utses myndigheter som ska vara behöriga att utfärda avlägsnandeorder och anmälningar, övervaka proaktiva åtgärder och fastställa påföljder. Det är upp till medlemsstaterna att bestämma hur många myndigheter de vill utse för dessa uppgifter.

(38) Påföljder är nödvändiga för att säkerställa att värdtjänstleverantörerna effektivt genomför sina skyldigheter enligt denna förordning. Medlemsstaterna bör anta bestämmelser om påföljder, även riktlinjer för bötfällning när så är lämpligt. Särskilt stränga påföljder ska fastställas om värdtjänstleverantören systematiskt underlåter att avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme från mottagandet av en avlägsnandeorder. Bristande efterlevnad i enskilda fall kan leda till påföljder, med respekt för principen *ne bis in idem* och proportionalitetsprincipen, samt med säkerställande av att påföljderna utdöms med beaktande av systematisk underlåtenhet. För att säkerställa rättssäkerhet bör det i förordningen anges i vilken utsträckning de relevanta skyldigheterna kan bli föremål för påföljder. Påföljder för bristande efterlevnad av artikel 6 bör endast tillämpas i fråga om skyldigheter som följer av en

begäran om rapportering enligt artikel 6.2 eller ett beslut om införande av ytterligare proaktiva åtgärder enligt artikel 6.4. Vid fastställande av huruvida böter bör föreskrivas, bör vederbörlig hänsyn tas till leverantörens ekonomiska resurser. Medlemsstaterna ska säkerställa att påföljderna inte uppmuntrar till avlägsnande av innehåll som inte är terrorisminnehåll.

(39) Användningen av standardiserade mallar underlättar samarbete och informationsutbyte mellan behöriga myndigheter och tjänsteleverantörer, och gör det möjligt för dem att kommunicera snabbare och mer effektivt. Det är särskilt viktigt att säkerställa snabba åtgärder efter mottagandet av en avlägsnandeorder. Mallarna minskar översättningskostnaderna och bidrar till en hög kvalitetsstandard. Svarsformulär bör också möjliggöra ett standardiserat informationsutbyte, vilket är särskilt viktigt om tjänsteleverantörerna inte kan följa ordern. Autentiserade inlämningskanaler kan garantera att avlägsnandeordern är autentisk, liksom att datum och tidpunkt för sändande och mottagande av ordern är korrekt.

(40) För att vid behov möjliggöra snabba ändringar av innehållet i de mallar som ska användas vid tillämpningen av denna förordning, bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt delegeras till kommissionen med avseende på ändringar av bilagorna I, II och III till denna förordning. För att kunna ta hänsyn till den tekniska utvecklingen och utvecklingen av den relaterade rättsliga ramen, bör kommissionen också ges befogenhet att anta delegerade akter för att komplettera denna förordning med tekniska krav på de elektroniska medel som de behöriga myndigheterna ska använda för att översända avlägsnandeorder. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016[15]. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(41) Medlemsstaterna bör samla in information om genomförandet av lagstiftningen. Ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter bör fastställas som underlag för en utvärdering av lagstiftningen.

(42) På grundval av resultaten och slutsatserna i genomföranderapporten och resultaten av övervakningen bör kommissionen genomföra en utvärdering av denna förordning tidigast tre år efter dess ikraftträdande. Utvärderingen bör bygga på de fem kriterierna effektivitet, ändamålsenlighet, relevans, samstämmighet och mervärde för EU. Man kommer att bedöma hur de olika operativa och tekniska åtgärder som föreskrivs i denna förordning fungerar, bland annat effektiviteten i de åtgärder som ska förbättra upptäckt, identifiering och avlägsnande av terrorisminnehåll, skyddsmekanismernas effektivitet samt inverkan på tredje parts potentiellt påverkade rättigheter och intressen, inklusive en översyn av kravet på att informera innehållsleverantörerna.

(43) Eftersom målet för denna förordning, nämligen att säkerställa att den digitala inre marknaden fungerar smidigt genom att förhindra spridning av terrorisminnehåll online, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och därför, på grund av begränsningens omfattning och verkningar, bättre kan uppnås på unionsnivå,

[15] EUT L 123, 12.5.2016, s. 1.

kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVSNITT I
ALLMÄNNA BESTÄMMELSER

Artikel 1
Syfte och tillämpningsområde

1. I denna förordning fastställs enhetliga regler för att förhindra att värdtjänster missbrukas för spridning av terrorisminnehåll online. Här fastställs i synnerhet följande:

   (a) Regler om aktsamhetskrav som värdtjänstleverantörer ska iaktta för att förhindra spridning av terrorisminnehåll via deras tjänster och vid behov säkerställa ett snabbt avlägsnande.

   (b) En rad åtgärder som medlemsstaterna ska vidta för att identifiera terrorisminnehåll, göra det möjligt för värdtjänstleverantörerna att snabbt avlägsna det samt underlätta samarbete med behöriga myndigheter i andra medlemsstater, med värdtjänstleverantörer och i tillämpliga fall med relevanta unionsorgan.

2. Denna förordning ska tillämpas på värdtjänstleverantörer som erbjuder tjänster i unionen, oberoende av deras huvudsakliga verksamhetsställe.

Artikel 2
Definitioner

I denna förordning gäller följande definitioner:

(1) *värdtjänstleverantör*: en leverantör av informationssamhällets tjänster som innebär att leverantören lagrar information som tillhandahållits av innehållsleverantören på dennas begäran och gör den lagrade informationen tillgänglig för tredje part.

(2) *innehållsleverantör*: en användare som har tillhandahållit information som lagras eller har lagrats av en värdtjänstleverantör på användarens begäran.

(3) *erbjuda tjänster i unionen*: göra det möjligt för juridiska eller fysiska personer i en eller flera medlemsstater att använda de tjänster som erbjuds av en värdtjänstleverantör som har en betydande anknytning till den eller de medlemsstaterna, såsom att värdtjänstleverantören

   (a) har ett verksamhetsställe i unionen,

   (b) har ett betydande antal användare i en eller flera medlemsstater,

   (c) riktar verksamheten till en eller flera medlemsstater.

(4) *terroristbrott*: brott enligt definitionen i artikel 3.1 i direktiv (EU) 2017/541.

(5) *terrorisminnehåll*: information som

(a) uppviglar till eller förespråkar, även genom förhärligande, utförande av terroristbrott, och därigenom ger upphov till en risk för att sådana handlingar utförs, och/eller

(b) uppmuntrar bidrag till terroristbrott, och/eller

(c) främjar en terroristgrupps verksamhet, i synnerhet genom att uppmuntra till deltagande i eller stöd till en terroristgrupp i den mening som avses i artikel 2.3 i direktiv (EU) 2017/541, och/eller

(d) lär ut metoder eller tekniker för att utföra terroristbrott.

(6) *spridning av terrorisminnehåll*: att göra terrorisminnehåll tillgängligt för tredje part via värdtjänstleverantörernas tjänster.

(7) *användarvillkor*: alla krav, villkor och klausuler som, oberoende av deras namn eller form, reglerar avtalsförhållandet mellan värdtjänstleverantören och dess användare.

(8) *anmälan*: ett meddelande från en behörig myndighet, eller i tillämpliga fall ett relevant unionsorgan, till en värdtjänstleverantör om information som kan anses vara terrorisminnehåll, för att leverantören på frivillig basis ska överväga om innehållet är förenligt med dess egna användarvillkor som syftar till att förhindra spridning av terrorisminnehåll.

(9) *huvudsakligt verksamhetsställe*: det huvudkontor eller säte där de huvudsakliga finansiella funktionerna och den operativa ledningen utövas.

AVSNITT II
Åtgärder för att förhindra spridning av terrorisminnehåll online

Artikel 3
Aktsamhetskrav

1. Värdtjänstleverantörer ska vidta lämpliga, rimliga och proportionella åtgärder i enlighet med denna förordning för att motverka spridning av terrorisminnehåll och skydda användarna mot terrorisminnehåll. När de gör detta ska de handla på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt, med vederbörlig hänsyn till användarnas grundläggande rättigheter och med beaktande av den grundläggande vikten av yttrandefrihet och informationsfrihet i ett öppet och demokratiskt samhälle.

2. Värdtjänstleverantörer ska i sina användarvillkor inbegripa bestämmelser för att förhindra spridning av terrorisminnehåll och tillämpa dessa.

Artikel 4
Avlägsnandeorder

1. Den behöriga myndigheten ska ha befogenhet att utfärda ett beslut som kräver att värdtjänstleverantören avlägsnar terrorisminnehåll eller gör det oåtkomligt.

2. Värdtjänstleverantörer ska avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme från mottagandet av avlägsnandeordern.

3. Avlägsnandeorder ska innehålla följande uppgifter i enlighet med mallen i bilaga I:

(a) Uppgift om den behöriga myndighet som utfärdat avlägsnandeordern och den behöriga myndighetens autentisering av avlägsnandeordern.

(b) En redogörelse av orsaker till att innehållet anses vara terrorisminnehåll, åtminstone genom hänvisning till de kategorier av terrorisminnehåll som anges i artikel 2.5.

(c) En webbadress (URL) och, vid behov, ytterligare information som gör det möjligt att identifiera det innehåll som anmäls.

(d) En hänvisning till denna förordning som rättslig grund för avlägsnandeordern.

(e) Datum och tidpunkt för utfärdande.

(f) Information om värdtjänstleverantörens och innehållsleverantörens prövningsmöjligheter.

(g) I tillämpliga fall, beslutet att inte lämna ut information om att terrorisminnehåll avlägsnats eller gjorts oåtkomligt i den mening som avses i artikel 11.

4. På värdtjänstleverantörens eller innehållsleverantörens begäran ska den behöriga myndigheten lämna en detaljerad motivering, utan att det påverkar värdtjänstleverantörens skyldighet att följa avlägsnandeordern inom den tidsfrist som anges i punkt 2.

5. De behöriga myndigheterna ska rikta avlägsnandeordern till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den juridiska företrädare som värdtjänstleverantören har utsett enligt artikel 16 och överföra den till den kontaktpunkt som avses i artikel 14.1. Sådana order ska sändas på ett elektroniskt sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar att säkerställa autentisering av avsändaren, även att datum och tidpunkt för sändandet och mottagandet av ordern är korrekt.

6. Värdtjänstleverantörer ska bekräfta mottagandet och utan onödigt dröjsmål informera den behöriga myndigheten om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt, med angivelse av i synnerhet tidpunkten för åtgärden, med hjälp av mallen i bilaga II.

7. Om värdtjänstleverantören inte kan följa avlägsnandeordern på grund av force majeure eller faktisk omöjlighet som inte kan tillskrivas värdtjänstleverantören, ska den utan dröjsmål informera den behöriga myndigheten och förklara orsakerna till detta med hjälp av mallen i bilaga III. Den frist som anges i punkt 2 ska tillämpas så snart de angivna orsakerna inte längre föreligger.

8. Om värdtjänstleverantören inte kan följa avlägsnandeordern eftersom ordern innehåller uppenbara fel eller inte innehåller tillräcklig information för att verkställa den, ska värdtjänstleverantören informera den behöriga myndigheten utan dröjsmål och be om nödvändiga klargöranden med hjälp av mallen i bilaga III. Den frist som anges i punkt 2 ska tillämpas så snart klargörandet har lämnats.

9. Den behöriga myndighet som utfärdade avlägsnandeordern ska informera den behöriga myndighet som övervakar genomförandet av proaktiva åtgärder i enlighet med artikel 17.1 c när avlägsnandeordern vunnit laga kraft. En avlägsnandeorder vinner laga kraft när den inte har överklagats inom tidsfristen enligt tillämplig nationell rätt eller när den har bekräftats efter ett överklagande.

Artikel 5
Anmälningar

1. Den behöriga myndigheten eller det relevanta unionsorganet får göra en anmälan till en värdtjänstleverantör.

2. Värdtjänstleverantörer ska införa operativa och tekniska åtgärder som underlättar snabb utvärdering av innehåll som har anmälts av de behöriga myndigheterna, och i tillämpliga fall relevanta unionsorgan, för frivilligt övervägande.

3. Anmälan ska riktas till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den rättsliga företrädare som värdtjänstleverantören utsett enligt artikel 16 och överföras till den kontaktpunkt som avses i artikel 14.1. Sådana anmälningar ska sändas på elektronisk väg.

4. Anmälan ska innehålla tillräckligt detaljerad information, inklusive orsakerna till att innehållet anses vara terrorisminnehåll, en webbadress och, vid behov, ytterligare information som gör det möjligt att identifiera det anmälda terrorisminnehållet.

5. Värdtjänstleverantören ska, som en prioriterad fråga, bedöma det innehåll som anges i anmälan utifrån sina egna användarvillkor och besluta om den ska avlägsna innehållet eller göra det oåtkomligt.

6. Värdtjänstleverantören ska skyndsamt informera den behöriga myndigheten eller det relevanta unionsorganet om resultatet av bedömningen och tidpunkten för eventuella åtgärder som vidtagits till följd av anmälan.

7. Om värdtjänstleverantören anser att anmälan inte innehåller tillräcklig information för att bedöma det anmälda innehållet, ska den utan dröjsmål informera de behöriga myndigheterna eller det relevanta unionsorganet och ange vilka ytterligare upplysningar eller klargöranden som krävs.

Artikel 6
Proaktiva åtgärder

1. Värdtjänstleverantörer ska, när så är lämpligt, vidta proaktiva åtgärder för att skydda sina tjänster mot spridning av terrorisminnehåll. Åtgärderna ska vara verkningsfulla och proportionella, med beaktande av risken för och graden av utsatthet för terrorisminnehåll, användarnas grundläggande rättigheter och den grundläggande vikten av yttrandefrihet och informationsfrihet i ett öppet och demokratiskt samhälle.

2. När den behöriga myndighet som avses i artikel 17.1 c har informerats i enlighet med artikel 4.9, ska den begära att värdtjänstleverantören, inom tre månader efter mottagandet av begäran och därefter minst en gång om året, lämnar in en rapport om de specifika proaktiva åtgärder som den har vidtagit, även med hjälp av automatiska verktyg, i syfte att

   (a) förhindra att innehåll som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det anses vara terrorisminnehåll laddas upp på nytt,

   (b) upptäcka, identifiera och snabbt avlägsna terrorisminnehåll eller göra det oåtkomligt.

   En sådan begäran ska sändas till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den rättsliga företrädare som värdtjänstleverantören utsett.

   Rapporterna ska innehålla all relevant information som gör det möjligt för den behöriga myndighet som avses i artikel 17.1 c att bedöma om de proaktiva

åtgärderna är effektiva och proportionella samt utvärdera hur eventuella automatiska verktyg och mekanismer för mänsklig tillsyn och kontroll som använts fungerar.

3. Om den behöriga myndighet som avses i artikel 17.1 c anser att de proaktiva åtgärder som vidtagits och rapporterats enligt punkt 2 är otillräckliga för att minska och hantera risken för och graden av utsatthet, får den begära att värdtjänstleverantören vidtar ytterligare specifika proaktiva åtgärder. För detta ändamål ska värdtjänstleverantören samarbeta med den behöriga myndighet som avses i artikel 17.1 c i syfte att identifiera de särskilda åtgärder som värdtjänstleverantören ska införa samt fastställa centrala mål, riktmärken och tidsfrister för genomförandet.

4. Om en överenskommelse inte kan nås inom tre månader från begäran enligt punkt 3 får den behöriga myndighet som avses i artikel 17.1 c utfärda ett beslut om att föreskriva ytterligare specifika nödvändiga och proportionella proaktiva åtgärder. Beslutet ska särskilt ta hänsyn till värdtjänstleverantörens ekonomiska kapacitet samt sådana åtgärders inverkan på användarnas grundläggande rättigheter och den grundläggande vikten av yttrandefrihet och informationsfrihet. Ett sådant beslut ska sändas till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den rättsliga företrädare som tjänsteleverantören utsett. Värdtjänstleverantören ska regelbundet rapportera om genomförandet av de åtgärder som fastställts av den behöriga myndighet som avses i artikel 17.1 c.

5. En värdtjänstleverantör får när som helst begära att den behöriga myndighet som avses i artikel 17.1 c prövar och, när det är lämpligt, återkallar en begäran eller ett beslut enligt punkt 2, 3 respektive 4. Den behöriga myndigheten ska lämna ett motiverat beslut inom rimlig tid efter det att den har mottagit värdtjänstleverantörens begäran.

Artikel 7
Bevarande av innehåll och relaterade data

1. Värdtjänstleverantörer ska bevara terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder, en anmälan eller proaktiva åtgärder enligt artiklarna 4, 5 och 6, samt relaterade data som avlägsnats till följd av att terrorisminnehållet har avlägsnats, och som är nödvändigt för

   (a) administrativa eller rättsliga prövningsförfaranden,

   (b) förebyggande, upptäckt, utredning och lagföring av terroristbrott.

2. Det terrorisminnehåll och de relaterade data som avses i punkt 1 ska bevaras i sex månader. Terrorisminnehållet ska, på den behöriga myndighetens eller domstolens begäran, bevaras under en längre period om och så länge som det krävs för ett sådant pågående administrativt eller rättsligt prövningsförfarande som avses i punkt 1 a.

3. Värdtjänstleverantörer ska säkerställa att terrorisminnehåll och relaterade data som bevaras enligt punkterna 1 och 2 omfattas av lämpliga tekniska och organisatoriska skyddsåtgärder.

   Dessa tekniska och organisatoriska skyddsåtgärder ska säkerställa att det terrorisminnehåll och de relaterade data som bevaras endast åtkoms och behandlas för de syften som avses i punkt 1, samt säkerställa en hög säkerhetsnivå för de berörda personuppgifterna. Värdtjänstleverantörer ska vid behov se över och uppdatera dessa skyddsåtgärder.

AVSNITT III
SKYDDSÅTGÄRDER OCH ANSVARIGHET

Artikel 8
Transparenskrav

1. Värdtjänstleverantörer ska i sina användarvillkor fastställa sin strategi för att förhindra spridningen av terrorisminnehåll, när så är lämpligt även en meningsfull förklaring av hur proaktiva åtgärder, bland annat användningen av automatiska verktyg, fungerar.
2. Värdtjänstleverantörer ska offentliggöra årliga transparensrapporter om åtgärder som vidtagits för att förhindra spridningen av terrorisminnehåll.
3. Transparensrapporterna ska innehålla minst följande information:
   (a) Information om värdtjänstleverantörens åtgärder för att upptäcka, identifiera och avlägsna terrorisminnehåll.
   (b) Information om värdtjänstleverantörens åtgärder för att förhindra att innehåll som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det anses vara terrorisminnehåll laddas upp på nytt.
   (c) Mängd terrorisminnehåll som avlägsnats eller gjorts oåtkomligt efter avlägsnandeorder, anmälningar respektive proaktiva åtgärder.
   (d) Översikt och resultat av klagomålsförfaranden.

Artikel 9
Skyddsåtgärder avseende användningen och genomförandet av proaktiva åtgärder

1. När värdtjänstleverantörer använder automatiska verktyg enligt denna förordning avseende det innehåll som de lagrar, ska de tillhandahålla effektiva och lämpliga skyddsmekanismer för att säkerställa att beslut som fattas angående detta innehåll, i synnerhet beslut om att avlägsna innehåll som anses vara terrorisminnehåll eller göra det oåtkomligt, är korrekta och välgrundade.
2. Skyddsåtgärderna ska särskilt omfatta mänsklig tillsyn och kontroll, när detta är lämpligt och i alla händelser när det krävs en detaljerad bedömning av det relevanta sammanhanget för att avgöra om innehållet ska anses vara terrorisminnehåll eller inte.

Artikel 10
Klagomålsmekanismer

1. Värdtjänstleverantörer ska inrätta effektiva och tillgängliga mekanismer som gör det möjligt för innehållsleverantörer, vars innehåll har avlägsnats eller gjorts oåtkomligt till följd av en anmälan enligt artikel 5 eller av proaktiva åtgärder enligt artikel 6, att lämna in ett klagomål mot värdtjänstleverantörens åtgärd och begära att innehållet återställs.
2. Värdtjänstleverantörer ska omgående granska varje klagomål som de tar emot och återställa innehållet utan onödigt dröjsmål om det inte var berättigat att avlägsna innehållet eller göra det oåtkomligt. De ska informera klaganden om resultatet av granskningen.

Artikel 11
Information till innehållsleverantörer

1. Om värdtjänstleverantörer har avlägsnat terrorisminnehåll eller gjort det oåtkomligt, ska de tillhandahålla information till innehållsleverantören om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

2. På innehållsleverantörens begäran ska värdtjänstleverantören informera innehållsleverantören om orsakerna till att innehållet avlägsnades eller gjordes oåtkomligt och möjligheterna att bestrida beslutet.

3. Skyldigheten enligt punkterna 1 och 2 ska inte gälla om den behöriga myndigheten beslutar att orsakerna inte bör lämnas ut av hänsyn till allmän säkerhet, såsom förebyggande, utredning, upptäckt och lagföring av terroristbrott, under en så lång tid som det är nödvändigt, men inte längre än [fyra] veckor efter beslutet. I sådana fall ska värdtjänstleverantören inte lämna någon information om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

AVSNITT IV
Samarbete mellan behöriga myndigheter, unionsorgan och värdtjänstleverantörer

Artikel 12
De behöriga myndigheternas kapacitet

Medlemsstaterna ska säkerställa att deras behöriga myndigheter har den kapacitet och de resurser som krävs för att uppnå målen och fullgöra sina skyldigheter enligt denna förordning.

Artikel 13
Samarbete mellan värdtjänstleverantörer, behöriga myndigheter och i tillämpliga fall relevanta unionsorgan

1. De behöriga myndigheterna i medlemsstaterna ska informera, samordna sig med och samarbeta med varandra, och när så är lämpligt med relevanta unionsorgan såsom Europol, avseende avlägsnandeorder och anmälningar för att undvika dubbelarbete, öka samordningen och undvika att störa utredningar i andra medlemsstater.

2. De behöriga myndigheterna i medlemsstaterna ska informera, samordna sig med och samarbeta med den behöriga myndighet som avses i artikel 17.1 c och 17.1 d avseende åtgärder som vidtas i enlighet med artikel 6 och verkställighetsåtgärder enligt artikel 18. Medlemsstaterna ska se till att den behöriga myndighet som avses i artikel 17.1 c och 17.1 d förfogar över all relevant information. För detta ändamål ska medlemsstaterna sörja för lämpliga kommunikationskanaler eller mekanismer för att säkerställa att den relevanta informationen delas inom rimlig tid.

3. Medlemsstater och värdtjänstleverantörer får välja att använda särskilda verktyg, när så är lämpligt även sådana som inrättats av relevanta unionsorgan som t.ex. Europol, för att särskilt underlätta

   (a) handläggning och återkoppling avseende avlägsnandeorder enligt artikel 4,

   (b) handläggning och återkoppling avseende anmälningar enligt artikel 5,

   (c) samarbete i syfte att identifiera och genomföra proaktiva åtgärder enligt artikel 6.

4. Om värdtjänstleverantörer får kännedom om bevis för terroristbrott ska de omedelbart underrätta de myndigheter som är behöriga att utreda och lagföra brott i den berörda medlemsstaten eller kontaktpunkten i den mening som avses i artikel 14.2 i den medlemsstat där de har sitt huvudsakliga verksamhetsställe eller en rättslig företrädare. I tveksamma fall får värdtjänstleverantörerna vidarebefordra denna information till Europol för lämplig uppföljning.

Artikel 14
Kontaktpunkter

1. Värdtjänstleverantörer ska inrätta en kontaktpunkt, så att de kan ta emot avlägsnandeorder och anmälningar på elektronisk väg och säkerställa att de handläggs snabbt i enlighet med artiklarna 4 och 5. De ska säkerställa att denna information offentliggörs.

2. I den information som avses i punkt 1 ska det anges på vilket eller vilka av unionens officiella språk, i den mening som avses i förordning (EG) nr 1/58, kontaktpunkten kan kontaktas och ytterligare utbyten avseende avlägsnandeorder och anmälningar enligt artiklarna 4 och 5 ska äga rum. Detta ska omfatta åtminstone ett av de officiella språken i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare enligt artikel 16 är bosatt eller etablerad.

3. Medlemsstaterna ska inrätta en kontaktpunkt för att hantera begäranden om klargöranden och återkoppling avseende avlägsnandeorder och anmälningar som de har utfärdat. Information om kontaktpunkten ska offentliggöras.

AVSNITT V
GENOMFÖRANDE OCH VERKSTÄLLIGHET

Artikel 15
Jurisdiktion

1. Den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe ska ha jurisdiktion vid tillämpningen av artiklarna 6, 18 och 21. En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i en av medlemsstaterna ska anses lyda under jurisdiktionen i den medlemsstat där den rättsliga företrädare som avses i artikel 16 är bosatt eller etablerad.

2. Om en värdtjänstleverantör inte har utsett en rättslig företrädare ska samtliga medlemsstater ha jurisdiktion.

3. Om en myndighet i en annan medlemsstat har utfärdat en avlägsnandeorder enligt artikel 4.1 har den medlemsstaten jurisdiktion att vidta tvångsåtgärder i enlighet med sin nationella lagstiftning för att verkställa avlägsnandeordern.

Artikel 16
Rättslig företrädare

1. En värdtjänstleverantör som inte har något verksamhetsställe i unionen men som erbjuder tjänster i unionen ska skriftligen utse en juridisk eller fysisk person till sin rättsliga företrädare i unionen för mottagande, efterlevnad och verkställighet av avlägsnandeorder, anmälningar, begäranden och beslut som utfärdas av de behöriga

myndigheterna på grundval av denna förordning. Den rättsliga företrädaren ska vara bosatt eller etablerad i en av de medlemsstater där värdtjänstleverantören erbjuder tjänsterna.

2. Värdtjänstleverantören ska anförtro den rättsliga företrädaren mottagande, efterlevnad och verkställighet av avlägsnandeorder, anmälningar, begäranden och beslut som avses i punkt 1 på den berörda värdtjänstleverantörens vägnar. Värdtjänstleverantörer ska förse sin rättsliga företrädare med de befogenheter och resurser som krävs för att samarbeta med de behöriga myndigheterna och efterleva dessa beslut och order.

3. Den utsedda rättsliga företrädaren kan hållas ansvarig för bristande efterlevnad av skyldigheter enligt denna förordning, utan att det påverkar de skadeståndskrav och rättsliga åtgärder som kan inledas mot värdtjänstleverantören.

4. Värdtjänstleverantören ska underrätta den behöriga myndighet som avses i artikel 17.1 d i den medlemsstat där den rättsliga företrädaren är bosatt eller etablerad om utseendet. Information om den rättsliga företrädaren ska offentliggöras.

AVSNITT VI
SLUTBESTÄMMELSER

Artikel 17
Utseende av behöriga myndigheter

1. Varje medlemsstat ska utse den eller de myndigheter som är behörig att

   (a) utfärda avlägsnandeorder i enlighet med artikel 4,

   (b) upptäcka och identifiera terrorisminnehåll och anmäla terrorisminnehåll till värdtjänstleverantörer i enlighet med artikel 5,

   (c) övervaka genomförandet av proaktiva åtgärder i enlighet med artikel 6,

   (d) säkerställa att skyldigheterna enligt denna förordning efterlevs genom påföljder i enlighet med artikel 18.

2. Senast [*sex månader efter denna förordnings ikraftträdande*] ska medlemsstaterna underrätta kommissionen om de behöriga myndigheter som avses i punkt 1. Kommissionen ska offentliggöra underrättelsen och eventuella ändringar därav i *Europeiska unionens officiella tidning*.

Artikel 18
Påföljder

1. Medlemsstaterna ska fastställa regler om påföljder vid värdtjänstleverantörers överträdelser av skyldigheter enligt denna förordning och ska vidta alla åtgärder som krävs för att säkerställa att de tillämpas. Sådana påföljder ska begränsas till åsidosättande av skyldigheterna enligt

   (a) artikel 3.2 (värdtjänstleverantörernas användarvillkor),

   (b) artikel 4.2 och 4.6 (genomförande av och återkoppling om avlägsnandeorder),

   (c) artikel 5.5 och 5.6 (bedömning av och återkoppling om anmälningar),

   (d) artikel 6.2 och 6.4 (rapporter om proaktiva åtgärder och antagande av åtgärder efter ett beslut som föreskriver specifika proaktiva åtgärder),

(e) artikel 7 (bevarande av data),

(f) artikel 8 (transparens),

(g) artikel 9 (skyddsåtgärder i samband med proaktiva åtgärder),

(h) artikel 10 (klagomålsförfaranden),

(i) artikel 11 (information till innehållsleverantörer),

(j) artikel 13.4 (information om bevis på terroristbrott),

(k) artikel 14.1 (kontaktpunkter),

(l) artikel 16 (utseende av en rättslig företrädare).

2. Påföljderna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska senast den [*inom sex månader efter denna förordnings ikraftträdande*] till kommissionen anmäla dessa regler och åtgärder samt utan dröjsmål eventuella ändringar som påverkar dem.

3. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de fastställer påföljdernas typ och nivå, beaktar alla relevanta omständigheter, bland annat

(a) överträdelsens karaktär, allvar och varaktighet,

(b) om överträdelsen är avsiktlig eller har orsakats av vårdslöshet,

(c) tidigare överträdelser som den juridiska person som hålls ansvarig gjort sig skyldig till,

(d) den finansiella styrkan hos den juridiska person som hålls ansvarig,

(e) värdtjänstleverantörens vilja att samarbeta med de behöriga myndigheterna.

4. Medlemsstaterna ska säkerställa att en systematisk underlåtenhet att uppfylla skyldigheterna enligt artikel 4.2 blir föremål för böter på upp till 4 % av värdtjänstleverantörens totala omsättning under det senaste räkenskapsåret.

Artikel 19
Tekniska krav och ändringar av mallarna för avlägsnandeorder

1. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 20 för att komplettera denna förordning med tekniska krav på de elektroniska medel som de behöriga myndigheterna ska använda för översändande av avlägsnandeorder.

2. Kommissionen ska ha befogenhet att anta sådana delegerade akter för att ändra bilagorna I, II och III i syfte att effektivt åtgärda eventuella behov av förbättringar av innehållet i formulären för avlägsnandeorder och formulär som ska användas för att meddela att det är omöjligt att verkställa avlägsnandeordern.

Artikel 20
Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 19 ska ges till kommissionen tills vidare från och med den [*datum då denna förordning börjar tillämpas*].

3. Den delegering av befogenhet som avses i artikel 19 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt, ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 19 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 21
Övervakning

1. Medlemsstaterna ska samla in information från sina behöriga myndigheter och värdtjänstleverantörerna under deras jurisdiktion om de åtgärder som dessa har vidtagit i enlighet med denna förordning och sända informationen till kommissionen senast den [31 mars] varje år. Denna information ska omfatta följande:

   (a) Information om antalet utfärdade avlägsnandeorder och anmälningar, mängd terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt, inklusive tidsramarna för detta i enlighet med artiklarna 4 och 5.

   (b) Information om de specifika proaktiva åtgärder som vidtagits i enlighet med artikel 6, inklusive den mängd terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt och tidsramarna för detta.

   (c) Information om det antal klagomålsförfaranden som inletts och de åtgärder som vidtagits av värdtjänstleverantörerna i enlighet med artikel 10.

   (d) Information om antalet prövningsförfaranden som har inletts och beslut som fattats av den behöriga myndigheten i enlighet med nationell lagstiftning.

2. Senast [*ett år efter den dag då denna förordning börjar tillämpas*] ska kommissionen upprätta ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter. I övervakningsprogrammet ska det anges indikatorer, vilka metoder som ska användas för att samla in uppgifter och andra nödvändiga belägg och med vilka intervaller detta ska ske. Det ska anges vilka åtgärder kommissionen och medlemsstaterna ska vidta för att samla in och analysera uppgifterna och andra belägg för att övervaka framstegen och utvärdera denna förordning i enlighet med artikel 23.

Artikel 22
Genomföranderapport

Senast den ... [*två år efter denna förordnings ikraftträdande*] ska kommissionen lägga fram en rapport för Europaparlamentet och rådet om tillämpningen av denna förordning. Information om övervakning enligt artikel 21 och information som härrör från transparenskraven enligt artikel 8 ska beaktas i kommissionens rapport. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta denna rapport.

Artikel 23
Utvärdering

Tidigast [*tre år från och med den dag då denna förordning börjar tillämpas*] ska kommissionen göra en utvärdering av denna förordning och lägga fram en rapport för Europaparlamentet och rådet om tillämpningen av förordningen, inklusive om effektiviteten i skyddsmekanismerna. Vid behov ska rapporten åtföljas av förslag till rättsakter. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta denna rapport.

Artikel 24
Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den [6 månader efter ikraftträdandet].

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*