EU:s förordning om terrorisminnehåll på internet

– frågan om behörig myndighet

DELBETÄNKANDE AV
UTREDNINGEN OM
BEHÖRIG MYNDIGHET OCH
LÄMPLIGA SANKTIONER
ENLIGT EU:S FÖRORDNING OM
ATT HANTERA SPRIDNING AV
TERRORISMINNEHÅLL ONLINE

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:76

EU:s förordning om terrorisminnehåll på internet

– frågan om behörig myndighet

Delbetänkande av Utredningen om behörig myndighet och lämpliga sanktioner enligt EU:s förordning om att hantera spridning av terrorisminnehåll online

Stockholm 2021

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:76

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2021

ISBN 978-91-525-0215-0 (tryck)
ISBN 978-91-525-0216-7 (pdf)
ISSN 0375-250X

Till statsrådet Mikael Damberg

Regeringen beslutade den 15 april 2021 med anledning av den då kommande Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online att ge en särskild utredare i uppdrag att föreslå vilken myndighet som bör pekas ut som behörig myndighet i Sverige och föreslå ändringar och kompletteringar av svensk rätt (dir. 2021:24).

Lagmannen Johan Sjöö förordnades den 30 april 2021 att vara särskild utredare. Samma dag förordnades hovrättsassessorn Lina Molin som sekreterare i utredningen.

Härmed överlämnas delbetänkandet *EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet* (SOU 2021:76).

De återstående frågor som omfattas av uppdraget kommer att behandlas i det slutbetänkande som ska redovisas senast den 15 april 2022.

Malmö i september 2021

Johan Sjöö

/Lina Molin

Innehåll

Sammanfattning

EU har antagit en förordning om åtgärder mot spridning av terrorisminnehåll på internet (Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online). Förordningen innehåller flera nyheter. Bland annat införs en möjlighet för behöriga myndigheter i medlemsstaterna att utfärda avlägsnandeorder mot värdtjänstleverantörer. En avlägsnandeorder innebär att en värdstjänstleverantör måste avlägsna terrorisminnehåll eller göra sådant innehåll oåtkomligt i samtliga medlemsstater inom en timme från det att leverantören mottog ordern. Andra uppgifter som följer av förordningen är att de behöriga myndigheterna ges möjlighet att granska avlägsnandeorder som berör den egna medlemsstaten, att kontrollera att en värdtjänstleverantör som är exponerad för terrorisminnehåll vidtar specifika åtgärder och att besluta om sanktioner vid överträdelse av förordningen.

Förordningen förutsätter att samarbetet utvecklas mellan medlemsstaterna respektive mellan medlemsstaterna och Europol.

Förordningen ställer krav på att rätten till ett effektivt rättsmedel tillgodoses i medlemsstaterna. Det innebär till exempel att en avlägsnandeorder ska kunna överklagas till domstol i den medlemsstat där orden utfärdats.

Det framgår även att tillämpningen av förordningen inte ska medföra någon ändring av skyldigheten att respektera de rättigheter, friheter och principer som avses i artikel 6 i EU-fördraget eller påverka de grundläggande principer som rör yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald. Det senare innebär bland annat att material inte ska anses vara terrorisminnehåll om det sprids till allmänheten i utbildningssyfte, journalistiskt syfte, konstnärligt syfte, forskningssyfte eller i syfte att förhindra eller bekämpa terrorism. Det omfattar inte heller material som ger uttryck för polemiska eller kontroversiella åsikter inom ramen för den offentliga debatten.

Utredningens uppdrag är att ta ställning till om Polismyndigheten eller Säkerhetspolisen bör utses till behörig myndighet i Sverige, att föreslå vilka sanktioner som ska aktualiseras vid överträdelser av förordningen och att i övrigt lämna nödvändiga författningsförslag.

Utredningen har i denna del haft att överväga om Polismyndigheten eller Säkerhetspolisen ska utses till behörig myndighet. Det finns enligt utredningen skäl som talar både för och emot att utse respektive myndighet. Utredningen menar sammantaget att övervägande skäl talar för att Polismyndigheten är mest lämplig för uppdraget och föreslår därför att regeringen utser Polismyndigheten till behörig myndighet enligt förordningen.

Uppdraget i övrigt ska redovisas senast den 15 april 2022.

Summary

The EU has adopted a regulation concerning measures to counter the dissemination of terrorist content on the internet (Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online). The Regulation contains several new features. These include a possibility for competent authorities in the Member States to issue removal orders to hosting service providers. A removal order means that a hosting service provider must remove terrorist content or disable access to such material in all Member States within one hour of the provider's receipt of the order. Other tasks resulting from the Regulation are that the competent authorities are given the possibility to scrutinise removal orders that concern their own Member State, verify that a hosting service provider exposed to terrorist content takes specific measures and decide on penalties in the case of infringements of the Regulation.

The Regulation requires improved cooperation between the Member States, and between the Member States and Europol.

The Regulation requires that the right to an effective remedy is satisfied in the Member States. This means, for example, that it must be possible to appeal a removal order in a court in the Member State where the order was issued.

It is also stated that the application of the Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles referred to in Article 6 of the Treaty on European Union and shall apply without prejudice to fundamental principles relating to freedom of expression and information, including freedom and pluralism of the media. The latter means, among other things, that material should not be considered to be terrorist content if it is disseminated to the public for educational, journalistic, artistic or research purposes or for the purposes of preventing or countering

terrorism, including material which represents an expression of polemic or controversial views in the course of public debate.

The remit of the Inquiry is to determine whether the Swedish Police Authority or the Swedish Security Service should be designated as the competent authority in Sweden, propose which penalties are to arise in the case of infringements of the Regulation and otherwise submit necessary legislative proposals.

Regarding the first part of the remit, the Inquiry has found that there are arguments both for and against designating either agency as the competent authority in Sweden. However, the Inquiry considers that on balance there are more arguments indicating that the Swedish Police Authority is more suitable for the task and therefore proposes that the Government designate the Swedish Police Authority as the competent authority under the Regulation.

A report on the Inquiry's remaining tasks will be presented by 15 April 2022 at the latest.

1 Författningsförslag

1.1 Förslag till förordning om ändring i förordningen (2014:1102) med instruktion för Polismyndigheten

Härigenom föreskrivs att bilagan till förordningen (2014:1102) med instruktion för Polismyndigheten ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

Bilaga

Polismyndigheten ska upprätthålla funktionen.

– –

8. att vara kontaktpunkt för säkerställande av omedelbar hjälp enligt artikel 35 i Europarådets konvention om it-relaterad brottslighet (ETS 185). Förordning (2021:839).

	9. att vara behörig myndighet enligt artikel 12 i Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.

Denna förordning träder i kraft den 7 juni 2022.

2 Uppdraget och dess genomförande

2.1 Bakgrund

Den 15 april 2021 beslutade regeringen att ge en särskild utredare i uppdrag att överväga om Polismyndigheten eller Säkerhetspolisen bör utses till behörig myndighet enligt Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (fortsättningsvis TCO-förordningen eller förordningen), att föreslå vilka sanktioner som ska aktualiseras vid överträdelser av förordningen och att i övrigt lämna nödvändiga författningsförslag.

I detta delbetänkande lämnar utredningen förslag på vilken myndighet som bör utses till behörig myndighet enligt TCO-förordningen. Uppdraget i övrigt ska redovisas senast den 15 april 2022.

2.2 Uppdraget

TCO-förordningen innebär en skyldighet för EU:s medlemsstater att utse en eller flera behöriga myndigheter som ska anförtros befogenheter att genomföra de uppgifter som följer av förordningen för att förebygga spridning av terrorisminnehåll på internet. En behörig myndighet ska till exempel kunna utfärda en order till en värdtjänstleverantör med krav på att avlägsna eller göra visst terrorisminnehåll på internet oåtkomligt. Myndigheten ska även granska gränsöverskridande avlägsnandeorder som berör den egna medlemsstaten och övervaka att en värdtjänstleverantör som är exponerad för terrorisminnehåll vidtar specifika åtgärder. Myndigheten ska vidare ha befogenhet att påföra sanktioner vid överträdelser av vissa bestämmelser i förordningen.

Senast den 7 juni 2022 ska EU:s medlemsstater meddela Europeiska kommissionen vilken eller vilka myndigheter som utsetts till att vara behöriga myndigheter.

Utredningens direktiv anger att endast en myndighet bör vara behörig i Sverige eftersom det, för det fall en enda myndighet har samtliga befogenheter till sitt förfogande, skapas bättre förutsättningar för ett effektivt utövande av dem. Vidare framgår det av direktiven att utredningen, mot bakgrund av förordningens innehåll och de krav som förordningen kommer att ställa på den behöriga myndigheten, bör föreslå Polismyndigheten eller Säkerhetspolisen. Utredningen ska även överväga vilka författningsändringar och andra åtgärder som krävs för att den föreslagna myndigheten ska kunna tillämpa förordningen och vidta de effektiva och rättssäkra åtgärder som ankommer på en behörig myndighet enligt förordningen. Utredningens förslag ska utformas så att myndighetens administrativa börda inte ökar mer än nödvändigt. Sammanfattningsvis ska utredningen:

- ta ställning till om Polismyndigheten eller Säkerhetspolisen bör utses till behörig myndighet enligt förordningen, och
- lämna nödvändiga författningsförslag.

Utredningens uppdrag i denna del är att föreslå vilken myndighet som bör utses till behörig myndighet i Sverige. I nästa del av uppdraget kommer utredningen att överväga och föreslå vilka sanktioner som ska kunna aktualiseras vid överträdelser av förordningen, analysera i vilken utsträckning förordningen i övrigt medför behov av ändringar eller kompletteringar av svensk rätt och lämna nödvändiga författningsförslag.

Utredningens direktiv finns bifogade till betänkandet, bilaga 1, tillsammans med förordningen, bilaga 2.

2.3 Utredningens arbete

Utredningen påbörjade arbetet i april 2021. Utredningen har inhämtat underlag i form av offentliga utredningar, propositioner och publikationer från bland annat Centrum mot våldsbejakande extremism (CVE) och Totalförsvarets forskningsinstitut (FOI).

Utredningen har haft flertalet kontakter med företrädare för Polismyndigheten och Säkerhetspolisen. Vidare har utredningen inhämtat information och kunskap om ämnesområdet bland annat genom möten med företrädare för CVE och FOI.

Utredningen har följt det pågående arbetet med att genomföra TCO-förordningen i övriga medlemsstater bland annat genom att delta i EU-gemensamma workshops och ha direkta kontakter med representanter från andra medlemsstater för att efterhöra vilka överväganden som gjorts, och görs, i frågan om valet av behörig myndighet.

Utredningen har vidare hållit sig uppdaterad om det pågående lagstiftningsarbetet inom EU rörande förslagen till en ny förordning om en inre marknad för digitala tjänster, den så kallade Digital Services Act och en ny förordning om åtgärder mot spridning av sexuellt övergreppsmaterial, se vidare under avsnitt 3.4.

3 Terrorisminnehåll på internet

3.1 Bakgrund

Digitaliseringen

Den digitala utvecklingen har skapat möjligheter till snabb och enkel kommunikation mellan människor oavsett var de befinner sig i världen. Utvecklingen har gått fort. Antalet användare av internet uppskattades år 2018 till omkring 2,4 miljarder vilket då motsvarade en tredjedel av jordens befolkning. Förra året var den siffran 4,7 miljarder.[1]

Samtidigt som utvecklingen till övervägande del är positiv finns det en annan och mörkare sida. Enskilda individer och organisationer använder internet för att begå brott och för att sprida olika former av olagligt material. Olagligt material som sprids på internet kan innehålla allt från hatpropaganda och sexuellt övergreppsmaterial till det som i TCO-förordningen benämns *terrorisminnehåll.* Med terrorisminnehåll avses i huvudsak innehåll som sprids till ett potentiellt obegränsat antal människor och anstiftar till terroristbrott om det, direkt eller indirekt, genom förhärligande av terroristgärningar förespråkar utförandet av terroristgärningar och därigenom medför fara för att ett eller flera sådana brott kan begås. Det kan även vara innehåll som syftar till att värva en person eller en grupp människor att begå eller bidra till terroristbrott eller för att delta i en terroristorganisations verksamhet.[2]

För terrorister och våldsbejakande extremister kan spridning av material på internet tjäna flera syften. Genom internet kan en grupp eller en organisation på ett enkelt sätt nå ut och sprida sina åsikter, hot och såväl officiell som inofficiell propaganda till ett stort antal männi-

[1] Nationalencyklopedin, Internet (u.å.) www.ne.se/uppslagsverk/encyklopedi/l% C3%A5ng /internet (hämtad 2021-08-30).
[2] Definitionen av terrorisminnehåll finns i artikel 2.7 Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online. Se även avsnitt 4.4.

skor. Nya medlemmar kan rekryteras. Organisationer kan använda internet för att publicera instruktioner på hur man utför ett terrorattentat eller recept på tillverkning av bomber eller liknande hjälpmedel. Vidare kan en organisation använda internet för att finansiera sin verksamhet. Finansieringen kan ske på många olika sätt till exempel genom försäljning av föremål så som kläder, flaggor och böcker eller genom direkta donationer på en hemsida.[3]

Terrororganisationen Islamiska staten (IS) är en aktör som under lång tid använt internet för att sprida sin propaganda och har därigenom rekryterat människor över hela världen till organisationen. Under inledningen av kriget i Syrien spred IS på daglig basis bilder och filmer på internet av avrättningar och annat grovt våld men även av det vardagliga livet i områden som IS kontrollerade och av religiösa ceremonier. Propaganda har därtill i stor utsträckning vidareförmedlats genom internet av individer och grupper av anhängare världen över. Internet har varit ett verktyg som bidragit till att organisationen spridits över hela världen och, trots de territoriella nederlagen, alltjämt har ett stort antal anhängare.[4]

Spridning av terrorisminnehåll på internet

Europeiska kommissionen lade i december 2020 fram en särskild agenda för att samordna arbetet mot terrorism inom unionen; EU:s agenda för terrorismbekämpning. Agendan delar upp arbetet mot terrorism i fyra delområden; *förutse* som syftar till att förbättra underrättelsearbetet inom unionen, *förhindra* som innebär ett ökat arbete mot radikalisering och extremistiska ideologier, *skydda* som avser att minska sårbarheten på offentliga platser och kritiska infrastrukturer, samt slutligen *reagera*, som syftar till att skapa rättsliga förutsättningar att lagföra gärningspersoner och att skydda brottsoffer.[5]

Åtgärder mot spridning av olagligt terrorisminnehåll på internet är en aktuell fråga i unionen inom ramen för arbetet mot terrorism. Frå-

[3] Council of Europe Publishing, Cyberterrorism – the use of the Internet for terrorist purposes, 2007, s. 33.
[4] K. Cohen och L. Kaati, Digital Jihad – Propaganda from the Islamic State, Totalförsvarets forskningsinstitut, FOI-R--4645--SE, november 2018, s. 23 ff.
[5] Meddelande från Kommissionen till Europaparlamentet, Europeiska rådet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: En agenda för terrorismbekämpning för EU: förutse, förhindra, skydda, reagera. COM (2020)795 final av den 9 december 2020, s. 1 ff.

gan har särskilt kommit att aktualiseras efter de senaste årens terroristattacker som har utförts i Europa och som har haft digitala inslag.

De digitala inslagen kan bestå i att enskilda gärningspersoner radikaliserats genom material på internet före genomförandet av ett attentat, att en gärningsperson införskaffat instruktioner på internet eller att ett terrorattentat livesänds och glorifieras på internet.[6]

Även på nationell nivå är konsekvenserna av digitaliseringen en aktuell fråga. Säkerhetspolisen uppger i sin årsbok för 2020 att digitaliseringen gjort att extremistmiljöer blivit tillgängliga för fler och att ensamagerande personer i dag ses som det främsta attentatshotet i Sverige. Lägesbilden beskrivs på följande sätt:

> Det främsta attentatshotet bedöms komma från ensamagerande personer som utöver en ideologisk drivkraft, kan ha personliga skäl till sitt agerande. Ett attentat skulle sannolikt genomföras med ganska enkla medel. […] Digitaliseringen har gjort extremistmiljöerna globala och tillgängliga för fler. Nya digitala plattformar ger helt andra förutsättningar för kommunikation och möjligheter att hitta likasinnade. Ensamagerande gärningspersoner i Sverige kan i många fall ha haft stöd i form av instruktioner, tips och inspiration från andra någonstans i världen, även om de begår attentaten lokalt och på egen hand.[7]

3.2 Rättslig reglering för att förhindra spridning på internet

Arbetet inom EU med att förhindra och bekämpa spridningen av olagligt innehåll på internet har som nämnts ovan pågått under ett antal år, främst genom frivilliga samarbeten med de större värdtjänstleverantörerna och inom ramen för EU Internet Referral Unit (EU IRU).[8]

Viss unionslagstiftning som reglerar användningen av digitala tjänster och förekomsten av meddelanden på internet med uppmaning att begå terroristbrott finns sedan tidigare (se avsnitt 3.2.1). Den unions-

[6] Se till exempel Kaati m.fl., Digitalt slagfält – en studie av radikalnationalistiska digitala miljöer, FOI-R--4813--SE, oktober 2019, och Meddelande från Kommissionen till Europaparlamentet, Europeiska rådet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: En agenda för terrorismbekämpning för EU: förutse, förhindra, skydda, reagera. COM (2020)795 final av den 9 december 2020, s. 6 f.

[7] Säkerhetspolisens årsbok 2020, s. 49.

[8] Facebook, Microsoft, Twitter och YouTube skapade tillsammans med Europeiska kommissionen år 2015 en uppförandekod för att motverka olaglig hatpropaganda på internet se: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1937 (hämtad 2021-08-31). För mer information om EU IRU se avsnitt 3.3.1 och www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru (hämtad 2021-08-31).

lagstiftning som reglerar digitala tjänster är dock av äldre slag. Det pågår ett lagstiftningsarbete inom EU i syfte att reglera den inre marknaden för digitala tjänster och skapa bättre rättsliga förutsättningar att agera mot olagligt innehåll på internet. TCO-förordningen är ett resultat av det lagstiftningsarbetet. Ytterligare reglering på området är att vänta.

3.2.1 Digitala tjänster

I dag regleras den inre marknaden för digitala tjänster i vissa delar av 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).[9] Artikel 14 i direktivet reglerar värdtjänstleverantörers ansvar över innehåll som tjänstemottagare (användare) lagrar hos leverantören. Bestämmelsen utgår från att värdtjänstleverantörer inte är ansvariga för innehåll som användare lagrar hos leverantören. Ansvarsfriheten förutsätter dock att tjänsteleverantören inte har kännedom om någon olaglig verksamhet eller olagligt innehåll på tjänsten. Även om värdtjänstleverantören skulle få kännedom om olagligt innehåll kan leverantören undgå ansvar om den, så snart han eller hon får kännedom eller blir medveten om materialet, utan dröjsmål agerar för att avlägsna det eller göra det oåtkomligt.

På nationell nivå kan i detta sammanhang nämnas lagen (1998:112) om ansvar för elektroniska anslagstavlor. En elektronisk anslagstavla är en tjänst för elektronisk förmedling av meddelanden, till exempel ett diskussionsforum eller en kommentarsfunktion på en hemsida (1 §). Lagen innehåller en skyldighet för den som tillhandahåller en digital anslagstavla på internet att ta bort eller förhindra spridning av innehåll som en användare publicerar, om materialet *uppenbart* faller in under definitionen av något av de brott som räknas upp i lagens 5 §. I uppräkningen finns bland annat olaga hot, hets mot folkgrupp, olaga våldsskildring och offentlig uppmaning.

[9] Direktivet har genomförts i nationell rätt genom lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster.

3.2.2 Terrorism

EU har vidtagit straffrättsliga lagstiftningsåtgärder mot terrorism som i viss mån berör spridning av terrorisminnehåll på internet, till exempel 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 (terrorismdirektivet). I artikel 5 anges att medlemsstaterna ska vidta nödvändiga åtgärder för att säkerställa att spridande, eller tillgängliggörande för allmänheten på annat sätt, oavsett metod, såväl på som utanför internet, av ett meddelande i syfte att anstifta till terroristbrott utgör en straffbar gärning om den begås uppsåtligen, om detta handlande, direkt eller indirekt, till exempel genom förhärligande av terroristgärningar, förespråkar utförandet av terroristbrott och därigenom medför fara för att ett sådant brott begås.

Bestämmelsen i terrorismdirektivet har införlivats i svensk rätt genom kriminaliseringen av offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen). För offentlig uppmaning döms den som i ett meddelande till allmänheten uppmanar eller annars söker förleda till särskilt allvarlig brottslighet eller till samröre med en terroristorganisation, till fängelse i högst två år.

3.3 Frivilliga åtaganden för att förhindra spridning på internet

3.3.1 EU Internet Referral Unit

I Europeiska säkerhetsagendan från 2015[10] lyftes fram en rad åtgärder mot terrorism, organiserad brottslighet och it-brottslighet. Ett initiativ som togs upp i agendan rörde särskilt spridning av terrorisminnehåll på internet: *The EU Internet Referral Unit* (EU IRU). EU IRU inrättades 2015 med stöd av Europolförordningen[11] som en enhet inom Europol.

[10] Meddelande från Kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, Europeiska säkerhetsagendan, COM(2015) 185 final av den 28 april 2015.
[11] Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) (Europolförordningen).

EU IRU:s huvudsakliga uppgifter är:

- att bistå andra EU-institutioner med strategiska och operationella analyser,
- att identifiera terrorism- och våldsbejakande innehåll på internet, anmäla innehåll till värdtjänstleverantören som kan strida mot leverantörens användarvillkor och efterfråga borttagande,
- att identifiera och begära borttagande av innehåll som används av smugglingsnätverk för att locka migranter och flyktingar, samt
- att samverka med tech-industrin under avlägsnandeprocessen.[12]

EU IRU identifierar och tar emot information om innehåll på internet som uppfattas strida mot en värdtjänstleverantörs användarvillkor. Om EU IRU bedömer att innehållet strider mot den berörda värdtjänstleverantörens användarvillkor skickar EU IRU en anmälan till värdtjänstleverantören om att avlägsna innehållet. Värdtjänstleverantören är inte bunden av anmälan utan gör en självständig bedömning av om innehållet strider mot företagets användarvillkor och därmed bör tas bort. Förfarandet leder till att en stor mängd material avlägsnas från internet på frivillig väg. Från starten fram till december 2017 hade EU IRU identifierat och anmält över 42 000 fall av publicerat material till värdtjänstleverantörer på mer än 80 olika plattformar. Under förra året granskade EU IRU 16 763 publicerat material.[13] I genomsnitt avlägsnas 86 procent av det material som EU IRU identifierar som oförenligt med värdtjänstleverantörers användarvillkor.[14]

Här kan också nämnas att värdtjänstleverantörer i mycket stor utsträckning på eget initiativ tar bort innehåll från internet som de anser strider mot företagets användarvillkor.[15]

För svenskt vidkommande har det under utredningens arbete framkommit att varken Säkerhetspolisen eller Polismyndigheten informerar EU IRU om innehåll som respektive myndighet påträffar på internet. Säkerhetspolisen och Polismyndigheten har förklarat att innehåll som påträffas på internet och som kan antas vara olagligt främst tas

[12] www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru (hämtad 2021-09-14).
[13] Europol Consolidated Annual Activity Report 2020, CAAR 2020, s. 25.
[14] www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru (hämtad 2021-08-31).
[15] Se till exempel rapporten från Facebook; Community standards enforcement report https://transparency.fb.com/data/community-standards-enforcement/dangerous-organizations/facebook#CONTENT_ACTIONED (hämtad 2021-08-31).

om hand i den brottsutredande verksamheten eller som kunskapsunderlag i underrättelseverksamheten.

I kontakt med andra medlemsstater har utredningen erfarit att andra medlemsstater, däribland Danmark och Tyskland, samarbetar med EU IRU och har därtill inrättat nationella Internet Referral Units. Sverige har inte någon nationell Internet Referral Unit.

3.3.2 EU Internet Forum

Ytterligare ett initiativ som lades fram i Europeiska säkerhetsagendan från 2015 och som inrättades samma år är EU Internet Forum (EUIF). EUIF skapades för att motverka terroristgruppers missbruk av internet och utveckla ett samarbete mellan EU:s medlemsstater och tech-industrin för att gemensamt arbeta mot terrorism och våldsbejakande extremistiskt innehåll på internet. Flera av de största aktörerna på internet deltar i EUIF, bland annat Facebook, Microsoft, Twitter och YouTube. Inom ramen för det arbetet har aktörerna från tech-branschen skapat en gemensam databas (”database for hashes”) för att säkerställa att innehåll som avlägsnats förblir permanent och oåterkalleligt borttaget från internet. Aktörerna har samlat in och lagrar nu över 200 000 olika bilder, videos med mera i databasen.[16]

EUIF deltar även i arbetet med den unionslagstiftning som rör digitala tjänster och olagligt innehåll på internet och bistår medlemsstaterna i arbetet med genomförandet av TCO-förordningen.

3.3.3 The Christchurch Call for Action

I samband med terroristattentatet mot två moskéer i Christchurch, Nya Zeeland, 2019, mördades 51 personer och 50 personer skadades. Terrorattentatet livesändes av gärningsmannen och filmen blev snabbt viral. Innan den initiala filmen kunde tas bort hade den setts över 4 000 gånger.[17] Händelsen tydliggjorde hur snabbt terrorisminnehåll, i det här fallet ett pågående terrorattentat, kan spridas på internet.

På initiativ av premiärministern i Nya Zeeland och Frankrikes president, grundades efter attentatet *the Christchruch Call for Action*, en frivillig sammanslutning av stater, organisationer och tech-företag

[16] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009 (hämtad 2021-08-31).
[17] www.christchurchcall.com/ (hämtad 2021-08-31).

som arbetar mot förekomsten av terrorisminnehåll och våldsbejakande extremistiskt innehåll på internet. Många länder och flera stora plattformsföretag har anslutit sig, däribland Sverige.

3.3.4 EU:s krisprotokoll

Som en följd av Christchurch-initiativet antog EU inom ramen för EU Internet Forum, EU Crisis Protocol (på svenska EU:s krisprotokoll rörande gemensamma åtgärder mot viral spridning online av terrorism- och våldsbejakande extremistiskt innehåll, EU:s krisprotokoll). EU:s krisprotokoll är ett frivilligt samarbete inom EU som har till syfte att hindra och motverka viral spridning av terrorisminnehåll och våldsbejakande extremistiskt innehåll på internet i samband med en nära förestående, pågående eller nyligen inträffad terrorattack. Verktygen i krisprotokollet ska underlätta ett snabbt, gemensamt och gränsöverskridande samarbete mellan anslutna medlemsstater. Europol fungerar som koordinator för krisprotokollet. Europol tillsammans med Europeiska kommissionen leder arbetet med att utveckla rutiner och arbetssätt för tillämpning av protokollet.[18]

Det åligger de stater som deltar i samarbetet att utse en kontaktpunkt för samarbetet. Sverige är en av de stater som deltar i samarbetet och Polismyndigheten är nationell kontaktpunkt.[19] Uppdraget hanteras inom Polismyndighetens befintliga ekonomiska ramar. Vid Polismyndigheten utgör Single point of operational contact vid Nationella operativa avdelningen (SPOC Noa) och vakthavande befäl vid Noa (VB Noa) en larmfunktion som tar emot inkommande information som kan initiera EU:s krisprotokoll. Larmfunktionen har beredskap att ta emot information och material dygnet runt. När SPOC Noa tar emot information gör VB Noa en inledande bedömning av om materialet kräver omedelbara operativa polisiära åtgärder avseende ordning och säkerhet. Materialet lämnas sedan vidare till funktioner inom Polismyndigheten för bedömning av om krisprotokollet ska aktiveras. Polismyndighetens bedömning är då, enligt myndigheten, beroende av samverkan med Säkerhetspolisen. Beslut om att aktivera EU:s

[18] https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6009 och Meddelande från Kommissionen till Europaparlamentet, Europeiska rådet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: En agenda för terrorismbekämpning för EU: förutse, förhindra, skydda, reagera. COM (2020)795 final den 9 december 2020, s. 7.
[19] Regleringsbrev för budgetåret 2020 avseende Polismyndigheten, ändringsbeslut 2020-06-17, Ju2020/02353/PO och Ju2020/02336/LP(delvis).

krisprotokoll fattas normalt av chefen för Noa eller, om ett beslut krävs utanför kontorstid, av polischef i beredskap. I juni 2021 hade Polismyndigheten ännu inte tillämpat EU:s krisprotokoll vid något tillfälle.[20]

3.4 Framtida unionslagstiftning

I EU:s agenda för terrorismbekämpning från december 2020 framgår att området *förhindra* innebär att unionen ska arbeta för att motverka spridning av extremistiska ideologier på internet bland annat genom antagandet av TCO-förordningen och en rättsakt om en inre marknad för digitala tjänster, den så kallade *Digital Services Act*.[21]

Samtidigt med agendan lade Europeiska kommissionen också fram ett förslag till en ny förordning, Förslag till Europaparlamentets och rådets förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 2000/31/EG, COM(2020) 825 final av den 15 december 2020 (*Digital Services Act* [DSA]). DSA är tänkt att utgöra ett ramverk för gränsöverskridande digitala tjänster. Förordningen har till syfte att möta den utveckling av nya affärsmodeller och tjänster, såsom sociala nätverk och marknadsplatser online, som skett i tiden efter införandet av direktivet om elektronisk handel.

För leverantörer av förmedlingstjänster kommer förordningen att innebära att leverantörerna måste uppfylla vissa krav på tillbörlig aktsamhet gentemot tjänstemottagaren (användaren), i vilken grad är beroende av verksamhetens omfattning. Leverantörerna ska bland annat vidta åtgärder mot olagligt innehåll, utse eller inrätta en kontaktpunkt för direkt kommunikation med medlemsstaternas behöriga myndigheter, utse rättsliga företrädare, upprätta transparensrapporter och inrätta anmälnings- och åtgärdsmekanismer (se exempelvis artikel 10, 11, 13–14 och 17). Förordningen uppställer särskilda skyldighet för de leverantörer av förmedlingstjänster som har 45 miljoner eller fler aktiva tjänstemottagare inom unionen per månad (avsnitt 4). Dessa stora

[20] Polismyndigheten, Organisation av Polismyndighetens uppdrag som nationell kontaktpunkt för EU:s krisprotokoll, juni 2021.
[21] Meddelande från Kommissionen till Europaparlamentet, Europeiska rådet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: En agenda för terrorismbekämpning för EU: förutse, förhindra, skydda, reagera. COM (2020)795 final av den 9 december 2020, s. 6–7.

aktörer kommer därtill behöva utföra riskbedömningar av verksamheten, genomföra en årlig oberoende revision med mera.

När begreppet olagligt innehåll används i förslaget till DSA avses information som i sig eller genom att den hänvisar till en verksamhet, däribland försäljning av produkter eller tillhandahållande av tjänster, inte är förenlig med unionsrätten eller lagstiftningen i en medlemsstat, oavsett denna lagstiftnings exakta sakinnehåll eller art (artikel 2 (g)). Definitionen i förordningen innebär att bedömningen av om visst innehåll är olagligt sker med stöd av nationell eller unionsrättslig lagstiftning, till exempel med stöd av TCO-förordningen.

Förordningsförslaget innefattar även skyldigheter för medlemsstaterna. Varje medlemsstat ska utse en behörig myndighet och en digital samordnare för att samarbeta med övriga medlemsstater och för att övervaka att de leverantörer av förmedlingstjänster som är etablerade, eller vars rättsliga företrädare är etablerad eller bosatt i medlemsstaten, följer de förpliktelser som framgår av förordningen (artikel 38). En medlemsstat kan rikta föreläggande mot en leverantör om att vidta åtgärder mot olagligt innehåll eller ett föreläggande om tillhandahållande av information om en eller flera tjänstemottagare (artikel 8 och 9).

DSA är inte avsedd att påverka tillämpningen av TCO-förordningen. TCO-förordningen kommer att utgöra en speciallag i förhållande till DSA som ska vara ett generellt och övergripande ramverk för digitala tjänster (artikel 1.5).

Det pågår även arbete inom EU med att ta fram en särskild förordning som ska förhindra spridning av sexuellt övergreppsmaterial på internet. I det förslag som läggs fram i slutet av 2021 kommer det troligen att finnas vissa likheter med TCO-förordningen.

Ingen av dessa rättsakter har ännu antagits i EU. Det är därför sannolikt att de slutgiltiga versionerna inte till fullo överensstämmer med den redogörelse som gjorts ovan.

4 Uppdraget som behörig myndighet

4.1 Bakgrund

Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen) innehåller regler för att åtgärda missbruk av värdtjänster för spridning av terrorisminnehåll till allmänheten (artikel 1). Förordningens övergripande syfte så som det kommer till uttryck i första skälet är att säkerställa att den digitala inre marknaden fungerar smidigt i ett öppet och demokratiskt samhälle genom att motverka att värdtjänster missbrukas för terrorismändamål och att bidra till den allmänna säkerheten i hela unionen. Den digitala inre marknadens funktion bör förbättras genom en ökad rättssäkerhet för värdtjänstleverantörer och stärkt förtroende för onlinemiljön hos användarna, samt genom ett förbättrat skydd för yttrandefriheten, inbegripet friheten att ta emot och sprida information och idéer i ett öppet och demokratiskt samhälle och mediernas frihet och mångfald.

Förordningen antogs av Europaparlamentet och rådet den 29 april 2021 och ska tillämpas i alla medlemsstater från och med den 7 juni 2022. Senast samma dag, den 7 juni 2022, ska Sverige underrätta Europeiska kommissionen vilken myndighet som utsetts till behörig myndighet i Sverige.

Den fortsatta framställningen i detta avsnitt avser att sammanfatta innehållet i förordningen och vad det innebär att utses till behörig myndighet.

4.2 Förordningen i korthet

Förordningen innehåller en möjlighet för behöriga myndigheter i medlemsstaterna att utfärda en avlägsnandeorder mot värdtjänstleverantörer och att granska gränsöverskridande avlägsnandeorder.

En avlägsnandeorder är ett rättsligt bindande verktyg för att snabbt avlägsna eller göra innehåll på internet som bedöms utgöra terrorisminnehåll oåtkomligt i hela unionen. Innehåll som omfattas av en avlägsnandeorder ska normalt tas bort eller göras oåtkomligt av värdtjänstleverantören inom en timme från det att leverantören tog emot ordern.

En gränsöverskridande order är en order som utfärdats av en annan medlemsstat än den där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad. En gränsöverskridande order kan granskas, på begäran av en värdtjänst- eller innehållsleverantör eller på eget initiativ, av den behöriga myndigheten i den medlemsstat där den berörda värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad. En sådan granskning innebär en prövning av om avlägsnandeordern på ett allvarligt eller uppenbart sätt är oförenlig med förordningen eller de grundläggande rättigheter och friheter som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna (stadgan).

En värdtjänstleverantör som inte efterlever en avlägsnandeorder kan påföras sanktioner. Det åligger varje medlemsstat att fastställa nationella regler om sanktioner mot värdtjänstleverantörers överträdelser av vissa uppräknade bestämmelser i förordningen och att vidta alla åtgärder som krävs för att säkerställa att de tillämpas.

En värdtjänstleverantör kan anses exponerad för terrorisminnehåll om den till exempel mottagit två eller fler avlägsnandeorder under de senaste tolv månaderna. Förordningen innehåller då ett krav på att en värdtjänstleverantör som bedöms vara exponerade för terrorisminnehåll måste vidta specifika åtgärder för att förhindra spridning av terrorisminnehåll på internet. Den aktuella värdtjänstleverantören beslutar vilka specifika åtgärder som ska vidtas för att förhindra spridning. Den behöriga myndigheten har sedan i uppgift att kontrollera att värdtjänstleverantörens vidtagna åtgärder uppfyller de krav som anges i förordningen. Om åtgärderna inte anses tillräckliga kan myndigheten rikta ett beslut mot värdtjänstleverantören med krav på att vidta tillräckliga specifika åtgärder, fortfarande utan att ange vilka

specifika åtgärder som ska vidtas. Om värdtjänstleverantören inte efterlever ett sådant beslut kan myndigheten under vissa förutsättningar besluta om sanktioner mot leverantören.

4.3 Uppdraget som behörig myndighet

Innebörden av uppdraget som behörig myndighet framgår huvudsakligen av artiklarna 12–14 i förordningen. Där framgår att den behöriga myndigheten ska ges den behörighet och de resurser som behövs för att *utfärda avlägsnandeorder* enligt artikel 3 och *granska gränsöverskridande avlägsnandeorder* enligt artikel 4. Den behöriga myndigheten ska även *övervaka värdtjänstleverantörers genomförande av specifika åtgärder* enligt artikel 5 och *påföra värdtjänstleverantörer sanktioner* enligt artikel 18.

Myndigheten ska utföra sina uppgifter på ett objektivt och icke-diskriminerande sätt med fullständig respekt för grundläggande rättigheter. Myndigheten får inte efterfråga eller ta emot instruktioner från något annat organ när det gäller utförandet av uppgifter i artikel 12.1 (bland annat utfärdandet av avlägsnandeorder) (artikel 13). Artikel 13.2 innebär ett krav på att myndigheten ska vara oberoende i sin myndighetsutövning vilket uttrycks i artikeln genom ett förbud mot att efterfråga och ta emot instruktioner från något annat organ.[1]

Utförandet av uppgifterna bygger på att ett samarbete utvecklas mellan värdtjänstleverantörer, behöriga myndigheter i respektive medlemsstat och, i vissa fall, med Europol. Det framgår uttryckligen i artikel 14 att de behöriga myndigheterna ska utbyta information, samordna sig och samarbeta med varandra och, när så är lämpligt, med Europol, avseende avlägsnandeorder. Samarbetet är särskilt viktigt för att undvika dubbelarbete, förbättra samordningen och undvika att störa utredningar i andra medlemsstater.

De behöriga myndigheterna ska därutöver även samordna sig på motsvarande sätt med de andra medlemsstaternas behöriga myndigheter när det kommer till övervakning av värdtjänstleverantörers genomförande av specifika åtgärder och i fråga om att påföra sanktioner.

[1] Se även andra bestämmelser om oberoende och oavhängighet t.ex. artikel 228.3 och artikel 286.3 fördraget om Europeiska unionens funktionssätt (EUF-fördraget) som rör en Europeisk ombudsman respektive revisionsrätten samt artikel 38, 52 och 69 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Avlägsnandeorder (artikel 3)

En avlägsnandeorder som utfärdas av en behörig myndighet ska innehålla ett krav på berörd värdtjänstleverantör att avlägsna terrorisminnehåll eller göra det oåtkomligt i samtliga medlemsstater. När en avlägsnandeorder har utfärdats ska värdtjänstleverantören så snart som möjligt men senast inom en timme avlägsna eller göra innehållet oåtkomligt.

Om det inte är fråga om ett brådskande fall ska en värdtjänstleverantör som aldrig tidigare mottagit en avlägsnandeorder få information om tillämpliga förfaranden och tidsfrister minst tolv timmar innan avlägsnandeordern utfärdas av myndigheten.

En avlägsnandeorder ska utfärdas enligt den mall som finns fogad till förordningen och innehålla de uppgifter som framgår av artikel 3.4.

En avlägsnandeorder ska gå att överklaga. Värdtjänst- och innehållsleverantörer ska ges rätt till ett effektivt rättsmedel, vilket innebär en rätt att bestrida en avlägsnandeorder inför domstolarna i den medlemsstat som utfärdat avlägsnandeordern (artikel 9).

En avlägsnandeorder skickas till den kontaktpunkt som värdtjänstleverantören utsett. Ordern vinner laga kraft vid utgången av överklagandefristen om inget överklagande lämnats in i enlighet med nationell rätt eller vid bekräftelse efter ett överklagande.[2]

Gränsöverskridande avlägsnandeorder (artikel 4)

En behörig myndighet som utfärdar en avlägsnandeorder mot en värdtjänstleverantör som har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare bosatt eller etablerad i en annan medlemsstat ska skicka en kopia av avlägsnandeordern till den andra medlemsstatens behöriga myndighet.

En behörig myndighet som mottar en sådan kopia av en gränsöverskridande avlägsnandeorder har möjlighet att på eget initiativ inom 72 timmar från mottagandet granska ordern för att fastställa om den på ett allvarligt eller uppenbart sätt är oförenlig med förordningen eller de grundläggande rättigheter eller friheter som garanteras i stadgan. Om myndigheten konstaterar oförenlighet ska denne meddela

[2] Jfr den engelska lydelsen av artikel 3.9 "A removal order shall become final upon the expiry of the deadline for appeal where no appeal has been lodged in accordance with national law or upon confirmation following an appeal."

ett motiverat beslut inom samma tid. Innan ett sådant beslut meddelas ska dock den myndighet som utfärdade den ursprungliga ordern informeras om avsikten att meddela ett beslut om oförenlighet.

Även en berörd värdtjänst- eller innehållsleverantör kan initiera ett granskningsförfarande genom att lämna in en motiverad begäran till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där den rättsliga företrädaren är bosatt eller etablerad. Begäran ska lämnas in inom 48 timmar räknat från mottagandet av ordern (värdtjänstleverantören) respektive från när information därom mottagits (innehållsleverantören). Myndigheten ska sedan meddela ett motiverat beslut inom 72 timmar från mottagandet av begäran om granskning.

Även ett beslut som meddelas efter en granskning av en gränsöverskridande avlägsnandeorder ska kunna överklagas. Värdtjänst- och innehållsleverantörer ska ges rätt till ett effektivt rättsmedel inför domstolarna i den medlemsstat som meddelar beslutet (artikel 9).

Ett beslut om granskning av en gränsöverskridande avlägsnandeorder ska skickas till den behöriga myndigheten som utfärdade det ursprungliga beslutet, värdtjänsteleverantören, innehållsleverantören (när denne begärt granskning) och, i vissa fall, Europol.

Specifika åtgärder (artikel 5)

Den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad kan även meddela beslut om att en värdtjänstleverantör är exponerad för terrorisminnehåll. En värdtjänstleverantör kan anses exponerad för terrorisminnehåll om leverantören under de föregående tolv månaderna mottagit två eller flera avlägsnandeorder som vunnit lagakraft. Värdtjänstleverantören kan när som helst begära omprövning av ett beslut om exponering.

Anses en värdtjänstleverantör exponerad för terrorisminnehåll ska denne vidta specifika åtgärder för att skydda sina tjänster mot spridning av terrorisminnehåll till allmänheten. Det är värdtjänstleverantören som beslutar om vilka åtgärder som ska vidtas. Förordningen räknar upp ett antal exempel på åtgärder som kan utgöra specifika åtgärder:

- Lämpliga tekniska och operativa åtgärder eller lämplig teknisk och operativ kapacitet, såsom lämplig personalstyrka eller lämpliga tekniska medel för att identifiera och snabbt avlägsna terrorisminnehåll eller göra det oåtkomligt.
- Lättillgängliga och användarvänliga mekanismer varmed användare till värdtjänstleverantören kan rapportera eller flagga påstått terrorisminnehåll.
- Andra mekanismer för att öka medvetenheten om terrorisminnehåll på dess tjänster, såsom mekanismer för användarmoderering.
- Andra åtgärder som en värdtjänstleverantör anser vara lämpliga för att åtgärda tillgängligheten av terrorisminnehåll på dess tjänster.

Oberoende av vilka specifika åtgärder som en värdtjänstleverantör väljer att vidta måste samtliga åtgärder uppfylla följande krav:

- Åtgärderna ska på ett effektivt sätt minska graden av exponering för terrorisminnehåll hos värdtjänstleverantörens tjänster.
- Åtgärderna ska vara riktade och proportionella, med särskilt beaktande av hur hög graden av exponering för terrorisminnehåll är hos värdtjänstleverantörens tjänster samt värdtjänstleverantörens tekniska och operativa kapacitet och finansiella styrka samt antalet användare av värdtjänstleverantörens tjänster och den mängd innehåll som de tillhandahåller.
- Åtgärderna ska tillämpas med fullständigt beaktande av användarnas rättigheter och legitima intressen, särskilt användarnas grundläggande rättigheter vad gäller yttrande- och informationsfrihet, respekt för privatlivet samt skydd av personuppgifter.
- Åtgärderna ska tillämpas på ett omsorgsfullt och icke-diskriminerande sätt.

Om åtgärderna innebär användning av tekniska medel ska värdtjänstleverantörerna dessutom införa lämpliga och effektiva skyddsåtgärder, särskilt genom mänsklig tillsyn och kontroll, för att säkerställa att de är korrekta och för att undvika avlägsnande av material som inte är terrorisminnehåll.

Värdtjänstleverantören ska ge in en rapport till den behöriga myndigheten om vilka specifika åtgärder som vidtagits och avses att vidtas.

En sådan rapport ska ges in första gången tre månader efter ett beslut om exponering och därefter årligen.

Om den behöriga myndigheten inte anser att de åtgärder som värdtjänstleverantören vidtagit uppfyller ovan angivna krav ska myndigheten rikta krav mot värdtjänstleverantören att vidta nödvändiga åtgärder för att säkerställa att kraven i förordningen uppfylls. En värdtjänstleverantör som inte uppfyller kraven på specifika åtgärder kan påföras sanktioner (se nedan och artikel 18).

Sanktioner (artikel 18)

Den behöriga myndigheten ska också ges befogenhet att påföra en värdtjänstleverantör sanktioner vid överträdelse av vissa uppräknade bestämmelser i förordningen, till exempel om en värdtjänstleverantör inte följer en avlägsnandeorder. Sanktionerna ska vara effektiva, proportionerliga och avskräckande. Sanktionssystem ska utformas på nationell nivå i varje medlemsstat.

Medlemsstaterna ska säkerställa att den behöriga myndigheten, när den beslutar att en sanktion ska påföras och när den fastställer sanktioneras typ och nivå, beaktar alla relevanta omständigheter, inbegripet bland annat överträdelsens karaktär, allvar och varaktighet, om överträdelsen var avsiktlig eller orsakades av vårdslöshet, tidigare överträdelser som värdtjänstleverantören har gjort sig skyldig till och värdtjänstleverantörens finansiella styrka.

Övriga uppgifter

Den behöriga myndigheten ska utöver de uppgifter som redogjorts för ovan även sammanställa årliga transparensrapporter. I rapporten ska det framgå hur många avlägsnandeorder som myndigheten utfärdat, hur många beslut som tagits rörande specifika åtgärder, antalet beslut om sanktioner och hur många ärenden som överklagats (artikel 8).

4.4 Begreppet terrorisminnehåll

När den behöriga myndigheten ska tillämpa förordningen, till exempel i samband med utfärdande av avlägsnandeorder, är definitionen av *terrorisminnehåll* av central betydelse. Definitionen finns i artikel 2.7 i förordningen där det framgår att terrorisminnehåll avser material som:

a) anstiftar till begåendet av ett av de brott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541, om sådant material, direkt eller indirekt, såsom genom förhärligande av terroristgärningar, förespråkar begåendet av terroristbrott, och därigenom medför fara för att ett eller flera sådana brott kan begås,

b) värvar en person eller en grupp av personer för att begå något av de brott som anges i artikel 3.1 a–i i direktiv (EU) 2017/541 eller bidra till att något av dessa brott begås,

c) värvar en person eller en grupp av personer för att delta i en terroristgrupps verksamhet i den mening som avses i artikel 4 b i direktiv (EU) 2017/541,

d) tillhandahåller instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen eller om andra specifika metoder eller tekniker för begående av eller bidragande till begåendet av något av de terroristbrott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541,

e) utgör ett hot om begående av ett av de brott som avses i artikel 3.1 a– i i direktiv (EU) 2017/541.

I 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 (terrorismdirektivet) framgår definitionen av *terroristbrott* som TCO-förordningen hänvisar till vid flera tillfällen. I artikel 3 terrorismdirektivet framgår följande definition av terroristbrott.

1. Medlemsstaterna ska vidta nödvändiga åtgärder för att säkerställa att följande uppsåtliga gärningar, vilka till följd av sin art eller sitt sammanhang allvarligt kan skada ett land eller en internationell organisation, definieras som terroristbrott i enlighet med brotts-

beskrivningarna i nationell rätt när de begås i något av de syften som anges i punkt 2:

a) Angrepp mot en persons liv som kan leda till döden.

b) Allvarliga angrepp på en persons fysiska integritet.

c) Människorov eller tagande av gisslan.

d) Förorsakande av omfattande förstörelse av en statlig eller annan offentlig anläggning, ett transportsystem, infrastruktur, inbegripet informationssystem, en fast plattform belägen på kontinentalsockeln, en offentlig plats eller privat egendom, som sannolikt utsätter människoliv för fara eller förorsakar betydande ekonomiska förluster.

e) Kapning av luftfartyg, fartyg eller andra allmänna transportmedel eller godstransportmedel.

f) Tillverkning, innehav, förvärv, transport, tillhandahållande eller användning av sprängämnen eller vapen, inbegripet kemiska, biologiska, radiologiska eller nukleära vapen, samt forskning om och utveckling av kemiska, biologiska, radiologiska eller nukleära vapen.

g) Utsläpp av farliga ämnen eller orsakande av brand, översvämningar eller explosioner som utsätter människoliv för fara.

h) Störande eller avbrytande av försörjningen av vatten, elkraft eller andra grundläggande naturresurser, som utsätter människoliv för fara.

i) Olaglig systemstörning enligt vad som avses i artikel 4 i Europaparlamentets och rådets direktiv 2013/40/EU (19), i fall där artikel 9.3 eller 9.4 b eller c i det direktivet är tillämplig, och olaglig datastörning enligt vad som avses i artikel 5 i samma direktiv, i fall där artikel 9.4 c i det direktivet är tillämplig.

j) Hot om att begå någon av de gärningar som anges i leden a–i.

2. De syften som avses i punkt 1 är följande:

a) Injaga allvarlig fruktan hos en befolkning.

b) Otillbörligen tvinga ett offentligt organ eller en internationell organisation att utföra eller att avstå från att utföra en viss handling.

c) Allvarligt destabilisera eller förstöra de grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturerna i ett land eller i en internationell organisation.

Vid bedömningen av om visst material ska anses utgöra terrorisminnehåll enligt TCO-förordningen ska den behöriga myndigheten och värdtjänstleverantörerna enligt skäl 11 ta hänsyn till:

- karaktären och formuleringen av uttalanden,
- i vilket sammanhang uttalandena gjordes, och
- uttalandenas potential att få skadliga konsekvenser för människors säkerhet.

Viktiga faktorer vid bedömningen av om visst material är terrorisminnehåll är vidare om det producerats av, kan tillskrivas eller sprids på uppdrag av en person, grupp eller enhet som ingår i unionens förteckning över personer, grupper och enheter som är delaktiga i terroristgärningar och föremål för restriktiva åtgärder (skäl 11).

Visst innehåll på internet undantas från att anses som terrorisminnehåll och kan därför inte omfattas av en avlägsnandeorder. Det handlar om innehåll som sprids till allmänheten i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller i syfte att förhindra eller bekämpa terrorism, inbegripet material som ger uttryck för polemiska eller kontroversiella åsikter inom ramen för den offentliga debatten. Det ska göras en bedömning för att fastställa spridningens verkliga syfte och om materialet sprids till allmänheten för dessa syften. Förordningen innebär inte någon ändring av skyldigheten att respektera de rättigheter, friheter och principer som avses i artikel 6 i EU-fördraget och ska tillämpas utan att det påverkar tillämpningen av grundläggande principer som rör yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald.

I fall där innehållsleverantören har ett redaktionellt ansvar bör varje beslut om avlägsnande beakta de publicistiska normer som fastställs genom press- och medieregleringen i enlighet med unionsrätten, bland annat stadgan (skäl 12 och artikel 1.3).

4.5 Sammanfattning av uppdraget som behörig myndighet

Uppdraget som behörig myndighet kan delas upp i två delar. Den första delen har en närmare koppling till det brottsbekämpande arbetet och avser möjligheten att utfärda avlägsnandeorder och att i vissa fall granska gränsöverskridande avlägsnandeorder. En order avser material som redan har spridits till allmänheten på internet och syftar till att se till värdtjänstleverantörer snabbt avlägsnar eller gör materialet oåtkomligt på internet och därigenom förhindrar ytterligare spridning.

Den andra delen av uppdraget som behörig myndighet är av mer administrativ karaktär där myndigheten har en funktion gentemot värdtjänstleverantörer som är exponerade för terrorisminnehåll att säkerställa att de vidtar tillräckliga åtgärder för att förhindra fortsatt eller framtida spridning av terrorisminnehåll. Till det kommer även möjligheten att påföra värdtjänstleverantörer sanktioner vid överträdelse av vissa bestämmelser i förordningen.

Slutligen finns det krav på rapportering gentemot Europeiska kommissionen.

5 Valet av behörig myndighet

5.1 Allmänna utgångspunkter

Utredningen har fått i uppdrag att överväga om antingen Polismyndigheten eller Säkerhetspolisen bör utses till behörig myndighet för Sveriges räkning. En utgångspunkt i utredningens direktiv är att endast en myndighet ska vara behörig myndighet. Som nämnts tidigare arbetar varken Polismyndigheten eller Säkerhetspolisen med avlägsnande av terrorisminnehåll på internet på det sätt som förordningen innebär. För utredningens överväganden är det därför av intresse att ge en översiktlig bild av Polismyndighetens och Säkerhetspolisens uppdrag och samarbeten i dag, att beskriva hur det övergripande ansvaret för terrorbekämpning är fördelat i Sverige och slutligen att göra en mindre utblick i EU genom en redogörelse för vilka nationella myndigheter några andra medlemsstater överväger att utse.

5.2 Arbetet med terrorbekämpning i Sverige

Säkerhetspolisen har ansvaret för terrorbekämpning i Sverige. Det terrorbekämpande arbetet består i att förebygga och förhindra att terrorattentat och annan terrorrelaterad brottslighet begås i landet och att utreda och beivra sådan brottslighet.[1]

Den straffrättsliga ram som reglerar arbetet mot terrorism finns bland annat i lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall (finansieringslagen), lagen (2003:148) om straff för terroristbrott och lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen).

[1] Se 3 § polislagen (1984:387), 3 § förordning (2014:1103) med instruktion för Säkerhetspolisen och www.sakerhetspolisen.se/kontraterrorism.html (hämtad 2021-08-31).

Regeringen beslutade 2015 om en nationell strategi mot terrorism som berör myndigheter och andra aktörer som på olika sätt kommer i kontakt med terrorismrelaterade frågor. Strategin understryker vikten av samverkan mellan olika aktörer i samhället och anger:

> Bekämpning av terrorism är ett ansvar för hela samhället. Terrorismen utvecklas ständigt och innebär nya utmaningar i arbetet med att bekämpa den. Alla som kan ha en roll i det arbetet måste ta ansvar för att bidra med det de kan. Samverkan är en förutsättning för att arbetet ska bli framgångsrikt.[2]

Strategin är utgångspunkten för Sveriges långsiktiga arbete mot terrorism både nationellt och internationellt. I korthet innehåller strategin åtgärder som kan kategoriseras i tre områden; förebygga, förhindra och försvåra. Inom området *förebygga* ligger fokus på att motverka radikalisering och rekrytering till extremist- och terroristgrupper och att påverka individers avsikt att begå eller stödja terrorismrelaterad brottslighet. *Förhindra* syftar till att motverka och minska förmågan och möjligheten att begå terroristattentat. Slutligen området *försvåra* handlar om att skapa och upprätthålla skydd för individer och minska samhällets sårbarhet för terroristattentat.[3]

Polismyndigheten deltar i arbetet mot terrorism och våldsbejakande extremism. I detta arbete utgår Polismyndigheten från den nationella strategin mot terrorism.[4] Polismyndigheten kan till exempel, efter en särskild överenskommelse med Säkerhetspolisen, ges ansvaret för en brottsutredning av ett inträffat terrorattentat i Sverige som innebär dödligt våld, skada på person eller stor materiell förstörelse och som är av sådan karaktär att det krävs omfattande utredningsresurser över tid.[5]

Polismyndigheten arbetar även mot penningtvätt och finansiering av terrorism. Myndigheten har inom det området ansvar för en samordningsfunktion för åtgärder mot penningtvätt och finansiering av terrorism. Funktionen består av representanter från ett antal olika

[2] Förebygga, Förhindra, Försvåra. Den svenska strategin mot terrorism. Regeringens skrivelse 2014/15:146, s. 41.
[3] Förebygga, Förhindra, Försvåra. Den svenska strategin mot terrorism. Regeringens skrivelse 2014/15:146, s. 1. Jfr även Meddelande från Kommissionen till Europaparlamentet, Europeiska rådet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: En agenda för terrorismbekämpning för EU: förutse, förhindra, skydda, reagera. COM (2020)795 final av den 9 december 2020.
[4] Polismyndighetens Årsredovisning 2020, s. 53.
[5] Slutredovisning av regeringsuppdrag att säkerställa insatsförmågan, Polismyndigheten, Nationella operativa avdelningen, september 2019, s. 3 och Revidering av överenskommelsen från 2015, bilaga A3 (A396.040/2016) till ramöverenskommelse A002.347/2015, Polismyndigheten.

nationella myndigheter, däribland Säkerhetspolisen, och har i uppdrag att bland annat löpande identifiera, kartlägga och analysera riskerna och metoderna för finansiering av terrorism i Sverige och att sammanställa nationella riskbedömningar för penningtvätt respektive finansiering av terrorism.[6]

Uppdraget att säkerställa Polismyndighetens förmåga att möta kraven i den nationella strategin mot terrorism har fördelats till enheten Nationella taktiska rådet (NTR) vid Nationella operativa avdelningen (NOA). NTR bedriver strategisk förmågeutveckling utifrån aktuell hotbild samt nationella och internationella erfarenheter rörande terrorismbekämpning. Arbetet sker i nära samverkan med Säkerhetspolisen.[7]

Ett annat forum där både Säkerhetspolisen och Polismyndigheten är representerade är Samverkansrådet mot terrorism. Samverkansrådet mot terrorism är ett nationellt nätverk av 15 myndigheter som har inrättats på initiativ av Säkerhetspolisen. Rådet saknar ett formellt uppdrag men har ett uttalat stöd av regeringen. Arbetet går ut på att förbättra samarbetet mellan myndigheterna före, under och efter ett terrorattentat.[8]

5.3 Polismyndigheten

Polismyndigheten bedriver polisverksamhet. Polismyndighetens uppdrag och ansvar framgår främst av polislagen (1984:387) och förordningen (2014:1102) med instruktion för Polismyndigheten. Av 2 § polislagen följer att myndighetens huvudsakliga uppgift är att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten. Myndigheten ska också övervaka den allmänna ordningen och säkerheten, ingripa när störningar har inträffat, samt utreda och beivra brott som hör under allmänt åtal.

---

[6] Artikel 7.2 Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism , om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG, i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2018/843, 13 § förordningen (2009:92) om åtgärder mot penningtvätt och finansiering av terrorism och 35 a § förordningen (2014:1102) med instruktion för Polismyndigheten.

[7] Förebygga, Förhindra, Försvåra. Den svenska strategin mot terrorism. Regeringens skrivelse 2014/15:146, s. 42 och s 15ff.

[8] www.sakerhetspolisen.se/kontraterrorism/samverkansradet-mot-terrorism.html och Förebygga, Förhindra, Försvåra. Den svenska strategin mot terrorism. Regeringens skrivelse 2014/15:146, s. 42 och s. 15 ff.

Av samma lag framgår det i 6 § att Polismyndigheten och Säkerhetspolisen ska samarbeta med varandra och med åklagarmyndigheterna. I 26 § instruktionen för Polismyndigheten framgår även att Polismyndigheten ska samarbeta med Säkerhetspolisen i den utsträckning som behövs för att polisverksamheten ska kunna bedrivas effektivt. Polismyndigheten och Säkerhetspolisen ska vidare i samråd bestämma och fortlöpande utveckla formerna för samverkan och samordning.[9]

Nationella operativa avdelningen

Organisatoriskt är Polismyndigheten indelad i sju polisregioner som i sin tur är indelade i polisområden och lokalpolisområden. Därutöver finns ett antal nationella avdelningar, till exempel ovan nämnda Nationella operativa avdelningen (Noa). Noa har till syfte att inrikta polisverksamheten nationellt och internationellt samt att stödja polisregionerna i olika typer av verksamheter.[10] Vid Noa finns, såvitt nu är av särskilt intresse, en Single point of operational contact (SPOC). SPOC är en dygnet runt-bemannad mottagningsfunktion för inkommande och utgående ärenden kopplade till Polismyndighetens internationella samarbete inom till exempel Europol och Interpol samt helt nyligen även EU:s krisprotokoll. SPOC Noa har inte i uppdrag att granska eller bedöma information utan vidarebefordrar inkommande och utgående information. Jämte SPOC Noa finns det ett vakthavande befäl vid Noa (VB Noa) som är tjänsteman i beredskap. VB Noa samverkar med andra myndigheters och organisationers motsvarigheter både nationellt och internationellt.[11]

Inom Noa finns även ett nationellt it-brottscentrum som har kunskap om brottslighet på internet och en särskild funktion för samarbete med vissa värdtjänstleverantörer i brottsutredningar. Vid it-brottscentrum bedrivs sedan flera år ett nära samarbete med några av de större värdtjänstleverantörerna i världen. Samarbetet syftar till att ge Polismyndigheten tillgång till uppgifter för att kunna identifiera personer som misstänks för brott i onlinemiljön, till exempel utnyttjande av barn för sexuell posering, hets mot folkgrupp eller olaga hot som begås på internet eller i sociala medier. Det samarbete som Polismyn-

[9] Jfr 8 § förvaltningslagen (2017:900).
[10] https://polisen.se/om-polisen/organisation/ (hämtad 2021-08-31).
[11] Polismyndigheten, Organisation av Polismyndighetens uppdrag som kontaktpunkt för EU:s krisprotokoll, juni 2021, s. 4.

digheten utvecklat med ett antal värdtjänstleverantörer bygger bland annat på en möjlighet som följer av amerikansk lag att på frivillig basis lämna ut vissa mindre integritetskänsliga uppgifter om abonnemang, framför allt ip-adresser.

Samarbetet inom Europol och uppdraget som nationell Europolenhet

Vid Europols huvudkontor i Haag, Nederländerna, finns personal anställd direkt av Europol tillsammans med särskilda sambandsmän som är utsända av medlemsstaterna. Polismyndigheten har ett antal sambandsmän stationerade vid Europols huvudkontor. Även Säkerhetspolisen har en sambandsman vid Europol. Varje medlemsstat har en nationell enhet som är kontaktpunkt och sambandsorgan mellan Europol och medlemsstaternas myndigheter. Sambandsmännen vid huvudkontoret i Haag har till uppgift att genomföra informations- och underrättelseutbyte mellan Europol och de nationella enheterna.

I Sverige är Polismyndigheten nationell Europolenhet.[12] I uppdraget som nationell enhet tar Polismyndigheten emot och samordnar information som kommer in till myndigheten inom ramen för Europolsamarbetet. Informationen fördelas sedan vidare inom Polismyndigheten eller till den myndighet som ansvarar för aktuellt område, till exempel Säkerhetspolisen.[13]

5.4 Säkerhetspolisen

Säkerhetspolisen är Sveriges säkerhetstjänst. Myndigheten bedriver även polisverksamhet, till exempel när det gäller terrorism.[14] Säkerhetspolisens uppdrag och ansvar framgår främst av polislagen och förordning (2014:1103) med instruktion för Säkerhetspolisen.

Till Säkerhetspolisens uppgifter hör enligt 3 § polislagen bland annat att förebygga, förhindra och upptäcka brottslig verksamhet som inne-

[12] 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 och Förordning (2014:1102) med instruktion för Polismyndigheten, bilaga 1, p 1.
[13] Artikel 7 och 8 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.
[14] 1 § polislagen (1984:387) och 1 § förordning (2014:1103) med instruktion för Säkerhetspolisen.

fattar brott mot rikets säkerhet eller terrorbrott, utreda och beivra sådana brott, fullgöra uppgifter i samband med personskydd av bland annat den centrala statsledningen.

Att vara säkerhetstjänst och samtidigt bedriva polisverksamhet, är ovanligt ur ett internationellt perspektiv. Liknande uppdrag har dock säkerhetstjänsterna i våra grannländer Danmark, Finland och Norge.

Säkerhetspolisens verksamhet är uppdelad i säkerhetsskydd, kontraspionage, kontraterrorism, författningsskydd och personskydd. Arbetet med kontraterrorism innebär att Säkerhetspolisen arbetar för att förebygga och avslöja terrorism som riktas mot Sverige, svenska intressen i utlandet, eller utländska intressen i Sverige, terrorhandlingar i andra länder, förekomsten av internationella terrornätverks förgreningar i Sverige samt stöd och finansiering av terrorverksamhet.[15]

Säkerhetspolisen samarbetar med nationella myndigheter, organisationer och andra privata aktörer för att fullgöra sitt uppdrag. Samverkan sker även internationellt både bilateralt och multilateralt.

5.5 Vilka myndigheter överväger andra medlemsstater att utse?

För att skapa ett fullgott utredningsunderlag har utredning försökt att få en bild av vilka överväganden som görs i frågan om behörig myndighet i andra medlemsstater. Utredningen har inhämtat information genom direkta kontakter med företrädare för andra medlemsstater och genom att delta i digitala möten som genomförts av Europeiska kommissionen och EU Internet Forum.

Under den begränsade utredningstid som stått till förfogande har det framkommit att medlemsstaterna, liksom Sverige, arbetar aktivt med frågan men att merparten ännu inte har tagit slutlig ställning. Det har påverkat möjligheten att här redogöra för en aktuell och slutlig bild av medlemsstaternas uppfattning.

Vid en jämförelse med andra medlemsstater och Sverige bör det noteras att myndighetsstrukturerna skiljer sig åt inom EU. Det finns till exempel skillnader i hur de nationella polismyndigheterna och säkerhetstjänsterna organisatoriskt är placerade samt hur respektive myndighetsuppdrag är utformat. Som nämnts ovan är Sverige i viss

[15] Säkerhetspolisens årsbok 2020, s. 13 och 56.

mån unikt eftersom både Polismyndigheten och Säkerhetspolisen bedriver polisverksamhet.

Det har i samband med utredningens kontakter framkommit att Tyskland i ett initialt skede övervägde fyra alternativa myndigheter; Bundeskriminalamt (Federal Criminal Police Office, BKA), Bundesverwaltungsamt (Federal Office of Administration), Bundesamt für Justiz (Federal Office for Justice) och Die medienanstalten (Media Authorities of the Federal States). De senaste uppgifterna som utredningen tagit del av är att Tyskland nu överväger att utse BKA (Tysklands federala kriminalpolis) till behörig myndighet att utfärda avlägsnandeorder och granska gränsöverskridande avlägsnandeorder. När det kommer till befogenheter rörande tillsynen över specifika åtgärder och utfärdande av sanktioner överväger Tyskland att utse Federal Office of Justice, en myndighet under Justitiedepartementet som i dag tillämpar den tyska lagen NetzDG (Network Enforcement Act) och därför har erfarenhet av att besluta om sanktioner.

Nederländerna är en medlemsstat som har kommit långt i arbetet med att förbereda genomförandet av TCO-förordningen. Under utredningens arbete har det framkommit att Nederländerna avser att inrätta en administrativ myndighet som kommer att ha i uppgift att tillämpa både TCO-förordningen och den kommande förordningen om åtgärder mot spridning av sexuellt övergreppsmaterial på internet.

I kontakt med danska justitiedepartement har det framkommit att Danmark överväger att utse Politiets Efterretningstjeneste (PET) till behörig myndighet. PET är den danska säkerhetstjänsten och ansvarar för terrorbekämpning i Danmark. Inom PET finns redan i dag en nationell Internet Referral Unit som hanterar terrorisminnehåll på internet. PET är bemannad dygnet runt.

Spanien har uppgett att de under 2021 kommer att inrätta en nationell Internet Referral Unit som kommer att ha i uppgift att bistå de/n myndighet/er som utses till behörig myndighet för Spaniens räkning. Vilken myndighet som ska utses är ännu inte bestämt.

6 Överväganden

6.1 Behörig myndighet

Utredningens förslag: Polismyndigheten utses till behörig myndighet i Sverige enligt Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.

Av förordningen framgår att EU:s medlemsstater kan utse en eller flera behöriga myndigheter för tillämpningen av TCO-förordningen. Det är inte nödvändigt enligt förordningen att inrätta någon ny myndighet för uppdraget utan en medlemsstat kan anförtro ett befintligt organ de funktioner som följer av förordningen. Varje medlemsstat bestämmer hur många behöriga myndigheter som ska utses och om de ska vara administrativa, brottsbekämpande eller rättsliga.

Det framgår av utredningens direktiv att endast en myndighet bör vara behörig myndighet i Sverige eftersom det, för det fall en enda myndighet har samtliga befogenheter till sitt förfogande, skapas bättre förutsättningar för ett effektivt utövande av dem. Direktiven uppdrar åt utredningen att överväga om Polismyndigheten eller Säkerhetspolisen bör utses till behörig myndighet enligt TCO-förordningen.

Utredningens direktiv uppställer inget uttryckligt hinder mot att i vart fall överväga om någon annan myndighet än Polismyndigheten eller Säkerhetspolisen kan bedömas som lämplig för uppdraget. Under utredningens arbete har några andra myndigheter förts fram som tänkbara att utse, främst Myndigheten för samhällsskydd och beredskap (MSB), Centrum mot våldsbejakande extremism (CVE) och den ännu inte inrättade myndigheten för psykologiskt försvar. Uppdraget som behörig myndighet kommer att innebära en dygnet runt-beredskap och, särskilt när det kommer till utfärdande av avlägsnandeorder och granskning av gränsöverskridande avlägsnandeorder, ett nära samband

med straffrättsliga bedömningar (jfr förordningens definition av terrorisminnehåll). Utredningens bedömning är att inget av de alternativ till Polismyndigheten och Säkerhetspolisen som framkommit har de organisatoriska och kunskapsmässiga förutsättningar som krävs för uppdraget. De nämnda myndigheterna utgör därför inte något relevant alternativ.

Både Polismyndigheten och Säkerhetspolisen uppfyller de formella kraven i förordningen, under förutsättning att den myndighet som utses också får de befogenheter som krävs för att kunna utföra uppgifterna som följer av uppdraget. Utredningen kommer därför i det följande endast att bedöma vilken av dessa två myndigheter som är lämplig för uppdraget som behörig myndighet.

Utredningens bedömning av vilken av de två myndigheterna som bör utses grundas på de uppgifter och verksamhetsområden som Polismyndigheten och Säkerhetspolisen i dag ansvarar för och på om respektive myndighet har förmågan att bygga upp en ändamålsenlig och kostnadseffektiv verksamhet för att utföra de uppgifter som följer av förordningen.

Utredningen har samrått med Polismyndigheten och Säkerhetspolisen. Uppgifter har inhämtats om respektive myndighets inställning till att utses till behörig myndighet. Ingen av myndigheterna anser att de är lämpliga för uppdraget, främst därför att de anser att rollen som behörig myndighet ligger utanför respektive myndighets kärnuppdrag.

Utredningen instämmer i Polismyndighetens och Säkerhetspolisens bedömning att uppdraget, å ena sidan att utfärda och granska avlägsnandeorder och å andra sidan att utöva tillsyn över värdtjänstleverantörer, inte ligger helt i linje med något av de två utpekade myndigheternas uppdrag så som de ser ut i dag.

Det nationella ansvaret för terrorbekämpning

Förordningens huvudsakliga syfte är att förhindra spridning av *terrorism*innehåll på internet. I Sverige är det Säkerhetspolisen som har ansvaret för att förebygga, förhindra och utreda terrorismrelaterad brottslighet. Säkerhetspolisens ansvarsområde ligger därför i sak nära det som ett uppdrag som behörig myndighet enligt TCO-förordningen innebär.

Säkerhetspolisens uppdrag innebär bland annat att förhindra och förebygga attentat, finansiering, logistiskt stöd, utbildning, rekrytering och radikalisering. Genom ansvaret för terrorbekämpning har Säkerhetspolisen särskild kunskap och erfarenhet av tillämpningen av lagstiftningen på området och de straffrättsliga bedömningar som följer därav. Säkerhetspolisen har även kunskap och kompetens om terrororganisationer och dessas närvaro och spridning på internet.

För att förebygga, förhindra och utreda terrorism och terrorismrelaterad brottslighet arbetar Säkerhetspolisen tillsammans med andra myndigheter och organisationer, bland annat Polismyndigheten. Polismyndigheten har tilldelats flera uppdrag de senaste åren som berör terrorbekämpning. Polismyndigheten har numera en nationell samordningsfunktion för åtgärder mot penningtvätt och finansiering av terrorism och kan, efter ett särskilt beslut, bistå Säkerhetspolisen med polisiära insatser i samband med terrorismrelaterad brottslighet eller efter särskild överenskommelse leda utredningsarbetet vid allvarligare attentat. Polismyndigheten har även, vilket kommer att beröras mer nedan, utsetts till Sveriges kontaktpunkt enligt EU:s krisprotokoll som, likt TCO-förordningen, handlar om att förhindra spridning av terrorisminnehåll på internet – ett uppdrag som således är nära besläktat med uppdraget som behörig myndighet enligt TCO-förordningen.

Säkerhetspolisens ansvar för terrorbekämpning talar i och för sig för att Säkerhetspolisen bör utses till behörig myndighet enligt TCO-förordningen. Den ansvarsfördelningen medför dock inte, enligt utredningen, att det är uteslutet att Polismyndigheten kan komma i fråga för uppdraget. Det är utredningens uppfattning att det utifrån respektive myndighets uppdrag och ansvarsområde finns förutsättningar att utse såväl Säkerhetspolisen som Polismyndigheten till behörig myndighet.

Gränsöverskridande samarbete

Vid den praktiska tillämpningen av TCO-förordningen kommer det att vara viktigt att bygga upp ett fungerande gränsöverskridande samarbete med behöriga myndigheter i andra medlemsstater. Myndigheterna kommer att behöva samordna sitt arbete och samarbeta för att till exempel förhindra att flera avlägsnandeorder utfärdas mot samma

innehåll eller att en order påverkar en utredning i en annan medlemsstat. I dagsläget är det tänkt att kommunikation mellan de behöriga myndigheterna och mellan myndigheterna respektive värdtjänstleverantörer ska ske via it-systemet PERCI (Platforme Européen de Retraits de Contenus Illégaux sur Internet) som håller på att utvecklas inom Europol.

Både Polismyndigheten och Säkerhetspolisen har i dag ett aktivt gränsöverskridande samarbete med andra länder både inom och utanför EU. När det kommer till det brottsbekämpande samarbetet inom EU är det Polismyndigheten som ansvarar för det svenska deltagandet i Europol. Polismyndigheten har sambandsmän stationerade vid Europols huvudkontor och är utsedd till nationell Europolenhet. Härigenom har Polismyndigheten det huvudsakliga ansvaret för kontakter inom ramen för det brottsbekämpande samarbetet inom unionen.

Polismyndigheten har vidare genom SPOC Noa en sambandscentral för inkommande och utgående internationella ärenden. Som nämnts tidigare är funktionen bemannad dygnet runt och fungerar som en internationell nod för det svenska Europolsamarbetet och flera andra internationella polisiära samarbeten, till exempel Interpol och EU:s krisprotokoll. SPOC Noa tar emot all Europolrelaterad information och vidarebefordrar inkommande ärenden till rätt behörig myndighet, till exempel Säkerhetspolisen.

Polismyndigheten har således redan i dag upparbetade kanaler, såväl tekniska som fysiska, för internationellt samarbete bland annat genom arbetet i Europol.

EU Internet Referral Unit

Sedan några år har flera frivilliga insatser initierats för att förhindra spridning av olagligt innehåll på internet. Med stöd av Europolförordningen bedrivs sedan 2015 ett aktivt arbete vid EU Internet Referral Unit (EU IRU) för att förhindra spridning av terrorisminnehåll på internet. Arbetet är frivilligt så till vida att den slutliga bedömningen görs av den berörda värdtjänstleverantören. EU IRU är organisatoriskt en del av Europol. Enheten söker i onlinemiljöer och tar emot anmälningar från medlemsstater och andra aktörer om terrorisminnehåll på internet som uppfattas strida mot värdtjänstleverantörers användarvillkor. EU IRU anmäler till berörd värdtjänstleverantör att det

finns terrorisminnehåll. Leverantören bedömer i sin tur om innehållet strider mot leverantörens användarvillkor och om det ska avlägsnas. En sådan anmälan från EU IRU följs i stor utsträckning av värdtjänstleverantörer.

Under utredningens arbete har det framkommit att varken Polismyndigheten eller Säkerhetspolisen informerar EU IRU om material som kan antas utgöra terrorisminnehåll. Om Polismyndigheten eller Säkerhetspolisen påträffar olagligt innehåll på internet vidarebefordras informationen till den myndighet som ansvarar för berörd brottskatalog (jfr terrorismrelaterad brottslighet, olaga hot, hets mot folkbrott osv.) eller tas om hand på annat sätt i det brottsförebyggande och brottsutredande arbetet inom respektive myndighet. I stället för att informera EU IRU om visst innehåll på internet läggs fokus på att utreda brott eller att använda innehållet för att bygga upp kunskap inom myndigheten. Såvitt är känt informerar inte heller någon annan nationell myndighet EU IRU om innehåll som påträffas på internet. Utredningens slutsats är att Sverige inte aktivt använder sig av EU IRU överhuvudtaget.

Utöver möjligheten för medlemsstater att anmäla material som de påträffar på internet till EU IRU har flera medlemsstater även inrättat nationella Internet Referral Units (IRU). De länderna arbetar därför redan i dag med att få bort olagligt innehåll på internet på nationell nivå. Sådana nationella IRU finns till exempel i Danmark och Tyskland. Sverige har inte inrättat någon nationell IRU som arbetar med olagligt innehåll på internet.

TCO-förordningen kan i detta sammanhang sägas utgöra en rättslig ram som bygger vidare på de frivilliga insatser som redan vidtagits och alltjämt vidtas inom unionen. När TCO-förordningen börjar tillämpas kommer den inte att hindra EU IRU och enskilda medlemsstater att även i fortsättningen använda sig av ett system med frivilliga anmälningar (referrals). I samband med utredningens arbete har det framkommit att flera medlemsstater överväger att även i framtiden primärt använda anmälan som en frivillig väg att få bort olagligt innehåll från internet och endast utnyttja möjligheten till avlägsnandeorder när en värdtjänstleverantör till exempel inte följer en anmälan (jfr proportionalitetsprincipen) eller om det är fråga om terrorisminnehåll som innebär ett överhängande hot mot människors liv och hälsa.

EU:s krisprotokoll

EU:s krisprotokoll utgör ytterligare ett gränsöverskridande samarbete som innehåller åtgärder för att förhindra spridning av terrorisminnehåll på internet.

EU:s krisprotokoll har utarbetats med utgångspunkt i de erfarenheter som drogs efter Christchruch-attentatet på Nya Zeeland 2019 där gärningsmannen livesände attentatet och på så sätt spred materialet till ett stort antal människor.

Krisprotokollet har till syfte att hantera nära förestående, pågående eller nyligen inträffade ”virala kriser” och terrorattentat samt förhindra spridning av terrorisminnehåll på internet. Krisprotokollets tillämpningsområde träffar i stor utsträckning samma material som TCO-förordningen. I båda instrumenten har Europol en viktig roll. På flera punkter skiljer sig dock instrumenten åt. Krisprotokollet är ett frivilligt samarbete mellan anslutna medlemsstater. TCO-förordningen är en bindande rättsakt som ger möjlighet att utfärda rättsligt bindande avlägsnandeorder gentemot värdtjänstleverantörer. Tidsaspekten utgör en ytterligare skillnad. Ett ärende enligt EU:s krisprotokoll är till sin natur brådskande medan ett ärende enligt TCO-förordningen inte nödvändigtvis är brådskande i den meningen att det måste vara fråga om ett pågående eller nära förestående terrorattentat.

Polismyndigheten är nationell kontaktpunkt enligt EU:s krisprotokoll. Uppgiften som kontaktpunkt är fördelad till befintliga funktioner inom Noa (SPOC Noa och VB Noa) där det redan i dag finns en dygnet runt-beredskap för internationella ärenden, såsom Europolärenden.

Uppdraget som behörig myndighet

De initiala överväganden som gjorts ovan tydliggör att det finns både argument som talar för att Polismyndigheten bör utses och argument som talar för att Säkerhetspolisen är mest lämplig för uppdraget.

Varken Polismyndigheten eller Säkerhetspolisen arbetar sedan tidigare aktivt med att bedöma om visst innehåll på internet ska avlägsnas eller göras oåtkomligt. Polismyndigheten har visserligen utsetts till kontaktpunkt för EU:s krisprotokoll men protokollet har ännu inte tillämpats i praktiken. Polismyndigheten har dock erfarenhet av att utreda brott i samarbete med i vart fall några av de större värdtjänst-

leverantörerna som faller under TCO-förordningens tillämpningsområde.

Ingen av myndigheterna utövar i dag någon tillsyn över värdtjänstleverantörer. Inte heller finns det något etablerat frivilligt samarbete mellan respektive myndighet och värdtjänstleverantörer såvitt gäller terrorism som det finns i vissa andra länder. (Polismyndigheten har emellertid ett sådant samarbete såvitt avser annan typ av brottslighet, se avsnitt 5.3). Ingen av myndigheterna bidrar med material till EU IRU. Ett sådant samarbete med, och myndighetsutövning över, värdtjänstleverantörer som följer av TCO-förordningen kan uppfattas som främmande för båda myndigheterna. Säkerhetspolisen har till utredningen framfört synpunkten att det, mot bakgrund av säkerhetstjänstens uppdrag i övrigt, kan ifrågasättas om det från principiella utgångspunkter är lämpligt att myndigheten i beslut med stöd av TCO-förordningen bedömer gränser för tryck- och yttrandefriheten. Argumentet kan enligt utredningens mening göras gällande även vad gäller Polismyndigheten så som en brottsbekämpande myndighet, men med den skillnad att Polismyndigheten har en betydligt bredare verksamhet och ett uppdrag som innefattar myndighetsutövning inom många olika områden.

Organisatoriskt kan uppdraget som behörig myndighet kräva vissa förändringar och omprioriteringar av den myndighet som utses. Det är dock utredningens uppfattning att uppdraget inte innebär ett krav på att myndigheten ska inrätta någon form av spaningsfunktion för att aktivt söka efter terrorisminnehåll på internet. Den behöriga myndigheten bör i stället ha beredskap för att – dygnet runt – ta emot information om innehåll på internet som kan omfattas av TCO-förordningen från andra nationella eller internationella myndigheter eller privata aktörer. Funktionen bör även ha beredskap att dygnet runt utfärda avlägsnandeorder och ta emot och granska gränsöverskridande avlägsnandeorder. Polismyndigheten är, som framkommit tidigare, redan i dag utrustad med funktioner som hanterar en dygnet runt-beredskap. Om Polismyndigheten utses till behörig myndighet bör en sådan beredskap sannolikt kunna ta avstamp i hur myndigheten valt att organisera handläggningen av ärenden enligt EU:s krisprotokoll. Polismyndigheten har därtill upparbetade kanaler med Europol som är en relevant aktör vid tillämpningen av TCO-förordningen och även med vissa värdtjänstleverantörer.

Det är mot denna bakgrund utredningens bedömning att Polismyndighetens organisation och befintliga funktioner har bäst förutsättningar att utföra uppgifterna som följer av uppdraget som behörig myndighet.

Den framtida lagstiftningskontexten

Utredningens överväganden görs i ljuset av vad som i dag är känt om den framtida lagstiftningskontexten inom EU. TCO-förordningen kommer sannolikt att inom några år vara en av flera rättsakter som rör den inre marknaden för digitala tjänster. Annan speciallagstiftning rörande olagligt innehåll på internet håller på att utarbetas inom EU. Dessa framtida rättsakter kommer att på ett än mer naturligt sätt beröra Polismyndighetens kärnverksamhet. Ett exempel är det kommande förslaget till förordning om åtgärder mot spridning av sexuellt övergreppsmaterial på internet.

Även om sakfrågorna i kommande rättsakter kommer att skilja sig åt finns det fördelar med att samma myndighet ansvarar för tillämpningen av de förordningar som rör avlägsnande av olagligt innehåll på internet och som angränsar till straffrätten. Förordningarna kommer sannolikt att innebära liknande praktiskt arbete i fråga om förfaranden, myndighetsutövning och kontakter med värdtjänstleverantörer. Det nätverk som den behöriga myndigheten kommer att bygga upp genom tillämpningen av TCO-förordningen kommer att skapa förutsättningar för ett effektivt genomförande av kommande förordning/ar. Den framtida lagstiftningen inom EU talar därför också för att det är mest kostnadseffektivt om Polismyndigheten utses till behörig myndighet enligt TCO-förordningen.

Kunskap om terrorrelaterade frågor

Utredningen ser flera fördelar med att utse Polismyndigheten till behörig myndighet. Det som kan tala mot att utse Polismyndigheten är den särskilda kompetens som Säkerhetspolisen besitter ifråga om terroristorganisationer och därtill kopplade frågor. Utredningen anser dock att den bristen kan övervinnas genom att Säkerhetspolisen bidar med sin kompetens i de TCO-ärenden där Polismyndigheten behöver stöd. Kunskapsutbyte och samverkan sker redan i dag mel-

lan myndigheterna och har varit en förutsättning för beslutet att utse Polismyndigheten till nationell kontaktpunkt enligt EU:s krisprotokoll. Om en sådan samverkan kommer till stånd även inom ramen för TCO-förordningen innebär det inte att Säkerhetspolisen ska göra några bedömningar i det enskilda fallet eller lämna några instruktioner som påverkar Polismyndigheten i sin myndighetsutövning. Om Polismyndigheten utses till behörig myndighet bör Säkerhetspolisen inta en expertroll, eller rådgivande funktion, gentemot Polismyndigheten i TCO-ärenden. Polismyndigheten ges därigenom en möjlighet att inhämta kunskap och underlag från Säkerhetspolisen som kan utgöra grund för en självständig prövning av det innehåll som påträffats på internet. Inte enbart Säkerhetspolisen har kunskap av betydelse för att Polismyndigheten ska kunna göra bästa möjliga bedömningar. Även myndigheter som Totalförsvarets forskningsinstitut och Centrum mot våldsbejakande extremism har stora kunskaper om terrorrelaterat material på internet och kan bidra med expertis.

Det är utredningens uppfattning att en sådan ordning och kunskapsinhämtning inte påverkar Polismyndighetens oberoende och är förenlig med artikel 13.2 i TCO-förordningen. Säkerhetspolisen har ställt sig positiv till att på detta sätt bistå Polismyndigheten med kunskap och erfarenhet.

Utredningen har övervägt om en rådgivande arbetsuppgift bör anges i de nämnda myndigheternas instruktioner men har stannat vid att i nuläget inte lägga fram något sådant förslag. Allmänna bestämmelser om samverkan mellan myndigheterna finns redan, se avsnitt 5.3.

Sammanfattande slutsatser

Utredningen gör bedömningen att Polismyndigheten är den myndighet som är mest lämplig att utföra de uppgifter som åligger den behöriga myndigheten enligt TCO-förordningen. Polismyndigheten föreslås därför som behörig myndighet enligt TCO-förordningen. Uppdraget bör framgå av bilagan till förordningen (2014:1102) med instruktion för Polismyndigheten.

Författningsförslag rörande genomförandet av TCO-förordningen, eventuell reglering av samverkan och informationsdelning mellan Polismyndigheten och Säkerhetspolisen, hur sanktionssystem och rätten

till effektiva rättsmedel bör utformas samt utredningens uppdrag i övrigt kommer att läggas fram i slutbetänkandet.

6.2 Framtiden

Utredningens bedömning: Det kan finnas anledning att göra en översyn av den behöriga myndighetens uppdrag i samband med att annan unionslagstiftning som rör olagligt innehåll på internet antas inom EU.

Inom EU pågår arbete med att reglera den inre marknaden för digitala tjänster. Europeiska kommissionen lade i december 2020 fram ett förslag till en ny förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 2000/31/EG (Digital Services Act [DSA]). DSA avser att bidra till en korrekt fungerande inre marknad för förmedlingstjänster och fastställa enhetliga regler för en säker, förutsebar och förtroendeskapande onlinemiljö, där de grundläggande rättigheterna i stadgan skyddas på ett effektivt sätt. I slutet av 2021 förväntas även ett förslag till en ny förordning om åtgärder mot spridning av sexuellt övergreppsmaterial på internet. Vidare förs diskussioner om en förordning med åtgärder mot hatpropaganda på internet.

Av förslaget till DSA framgår att förordningen är tänkt att utgöra en ramlag i förhållande till annan unionslagstiftning. Så som förslaget ser ut vid tidpunkten för detta delbetänkande innehåller det, likt TCO-förordningen, ett krav på att utse en behörig myndighet för tillämpningen av förordningen och därutöver även en nationell digital samordnare. Förslaget till DSA innehåller också bestämmelser som rör avlägsnande av olagligt innehåll. Grunden för om ett visst innehåll ska anses vara olagligt föreslås dock inte följa direkt av DSA utan ska bedömas med tillämpning av annan unionslagstiftning eller nationell rätt, till exempel med stöd av TCO-förordningen eller den kommande förordningen om åtgärder mot spridning av sexuellt övergreppsmaterial på internet.

Om och när de rättsakter som rör digitala tjänster och avlägsnande av olagligt innehåll på internet antas inom EU kan det finnas anledning att göra en översyn av myndighetsstrukturen i Sverige rörande digitala tjänster och innehåll i onlinemiljön. I det skedet ser

utredningen fördelar med att lyfta bort de uppgifter i TCO-förordningen som är av mer tillsynskaraktär från Polismyndigheten till en annan administrativ myndighet.

En sådan förändring skulle kunna ske genom inrättande av en ny myndighet som får i uppdrag att utöva tillsyn över digitala tjänster och onlinemiljön eller genom att en befintlig myndighet tar över ansvaret för de uppgifterna.

Som framgått av avsnitt 5.5 har flera medlemsstater redan nu, inför ikraftträdandet av TCO-förordningen, planer på att dels inrätta särskilda myndigheter, dels att dela upp uppgifterna i förordningen på flera myndigheter.

7 Förslagets konsekvenser

En särskild utredare ska redovisa vilka konsekvenser i olika avseenden som förslagen i ett betänkande kan få (1 § andra stycket kommittéförordningen [1998:1474]). Enligt 14 § gäller att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller regioner ska utredaren föreslå en finansiering.

I 15 § anges att om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen ska konsekvenserna i det avseendet anges i betänkandet. Om ett betänkande innehåller förslag till nya regler ska, enligt 15 a §, förslagens kostnadsmässiga och andra konsekvenser anges i betänkandet.

I detta delbetänkande föreslår utredningen att Polismyndigheten ska utses till behörig myndighet i Sverige. Utredningen gör också bedömningen att Säkerhetspolisen och andra relevanta myndigheter kan komma att behöva bistå Polismyndigheten med kompetens i terrorismrelaterade frågor.

Hur stora konsekvenser uppdraget som behörig myndighet kommer att innebära i fråga om antal ärenden för Polismyndigheten är enligt utredningens bedömning omöjligt att uppskatta. TCO-förordningen har ännu inte börjat tillämpas i unionen. Någon motsvarande rättsakt finns inte sedan tidigare.

Antalet ärenden kommer att vara beroende av ett flertal faktorer som utredningen i dagsläget bedömer som osäkra. En faktor av bety-

delse är hur många värdtjänstleverantörer som kommer att anses etablerade i Sverige. En annan faktor är vilken ambitionsnivå den behöriga myndigheten kommer att arbeta utifrån, bland annat eftersom förordningen inte innebär något krav på att den behöriga myndigheten ska vara aktiv i sökandet efter terrorisminnehåll på internet. Andra faktorer som kommer att påverka mängden ärenden är i vilken utsträckning andra medlemsstater kommer att tillämpa förordningen och hur de kommer att förhålla sig till material som publiceras av innehållsleverantörer eller värdtjänstleverantörer som är etablerade i Sverige. Mängden gränsöverskridande avlägsnandeorder som utfärdas och som berör Sverige kommer att påverka arbetsbördan för den behöriga myndigheten. Här ska också tas i beaktande att flera medlemsstater överväger att även i framtiden använda möjligheten till *referrals*, dvs. frivilliga anmälningar till värdtjänstleverantörer om att avlägsna innehåll på internet. En sådan utveckling talar för att Sverige inte kommer att handlägga några större volymer av gränsöverskridande avlägsnandeorder.

Det saknas förutsättningarna för utredningen att nu göra en annan bedömning än att det nya uppdraget ryms inom Polismyndighetens befintliga ekonomiska ram. Utredningen ska emellertid i kommande del av uppdraget föreslå kompletterande nationella bestämmelser för tillämpningen av förordningen, vilket bland annat inkluderar bestämmelser rörande sanktioner vid överträdelse av förordningen och rätten till effektivt rättsmedel. Utredningen återkommer i slutbetänkandet med en detaljerad redogörelse för samtliga förslags konsekvenser, vilket även kan komma att inkludera konsekvenser av uppdraget som behörig myndighet.

Kommittédirektiv 2021:24

Behörig myndighet och lämpliga sanktioner enligt EU:s förordning om att hantera spridning av terrorisminnehåll online

Beslut vid regeringssammanträde den 15 april 2021

Sammanfattning

En särskild utredare ska med anledning av den kommande EU-förordning som ska hantera spridningen av terrorisminnehåll online föreslå vilken myndighet som bör pekas ut som behörig myndighet för Sveriges räkning och föreslå ändringar och kompletteringar av svensk rätt.

Utredaren ska bl.a.

- ta ställning till om Polismyndigheten eller Säkerhetspolisen bör utses till behörig myndighet enligt förordningen,
- föreslå vilka sanktioner som ska aktualiseras vid överträdelser av förordningen, och
- lämna nödvändiga författningsförslag.

Uppdraget att lämna förslag på behörig myndighet ska redovisas senast den 1 oktober 2021. Uppdraget i övrigt ska redovisas senast den 15 april 2022.

EU-förordningen

I december 2020 nåddes en överenskommelse mellan Europaparlamentet och rådet om en förordning om att hantera spridning av terrorisminnehåll online (förordningen). Förordningen förväntas beslutas inom kort.

Förordningen kommer att innehålla bestämmelser som syftar till att förebygga att terrorisminnehåll, såsom begreppet definieras i förordningen, sprids på internet och når allmänheten.

Förordningen kommer att innebära ett flertal skyldigheter för sådana aktörer som ska räknas som värdtjänstleverantörer enligt förordningen i den mån som de erbjuder sina tjänster inom EU. Värdtjänstleverantörer som enligt förordningen ska anses vara utsatta för terrorisminnehåll kommer bl.a. att åläggas skyldighet att vidta specifika åtgärder i syfte att skydda sina tjänster från spridning av terrorisminnehåll.

Medlemsstaterna är vidare skyldiga att utse en eller flera behöriga myndigheter som ska anförtros befogenheter att vidta vissa åtgärder för att förebygga spridning av terrorisminnehåll på internet. Var och en av medlemsstaterna ska också fastställa nationella bestämmelser om sanktioner vid värdtjänstleverantörers överträdelser av vissa skyldigheter enligt förordningen.

Förordningen kommer att träda i kraft 20 dagar efter att den har kungjorts och ska börja tillämpas tolv månader efter ikraftträdandet. Förordningen kommer vara direkt tillämplig i medlemsstaterna när den träder i kraft men kommer både möjliggöra och förutsätta kompletterande nationella bestämmelser när det gäller de skyldigheter som åligger medlemsstaterna.

Den nuvarande svenska regleringen

Enligt 2 kap. 1 § regeringsformen (RF) är var och en gentemot det allmänna tillförsäkrad yttrandefrihet, det vill säga frihet att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor (se även artikel 10 i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna och lagen [1994:219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna och jämför även 2 kap. 19 § RF). Av 1 kap. 1 § yttrandefri-

hetsgrundlagen (YGL) följer vidare att var och en gentemot det allmänna är tillförsäkrad rätt att i ljudradio, tv och vissa liknande överföringar, offentliga uppspelningar ur en databas samt filmer, videogram, ljudupptagningar och andra tekniska upptagningar offentligen uttrycka tankar, åsikter och känslor och i övrigt lämna uppgifter i vilket ämne som helst.

I 1 kap. 4 § YGL finns den s.k. databasregeln som under vissa förutsättningar ger grundlagsskydd för yttranden som sker på till exempel en webbplats. För vissa aktörer gäller grundlagsskyddet utan att någon särskild åtgärd behöver vidtas, däribland redaktioner för periodiska skrifter. Andra aktörer som publicerar sig på internet har möjlighet att ansöka om utgivningsbevis och på så sätt få ett s.k. frivilligt grundlagsskydd.

Att exempelvis en webbsida är grundlagsskyddad enligt YGL innebär bland annat att myndigheter inte får förhandsgranska eller försvåra publicering av innehåll på webbsidan. Ansvar för innehållet i en publicering får endast utkrävas efter publicering och ansvar kan bara komma i fråga för vissa uppräknade brott i YGL, däribland hets mot folkgrupp och uppvigling. Det är i första hand den ansvarige utgivaren som kan hållas ansvarig för innehållet på en grundlagsskyddad webbplats.

Lagen (1998:112) om ansvar för elektroniska anslagstavlor gäller för elektroniska anslagstavlor, det vill säga en tjänst för elektronisk förmedling av meddelanden. Lagen gäller inte för sådana tjänster som skyddas av YGL. Av 5 § första stycket samma lag följer att den som tillhandahåller en elektronisk anslagstavla har en skyldighet att ta bort vissa meddelanden från tjänsten eller på annat sätt förhindra vidare spridning av meddelandet, om meddelandets innehåll uppenbart är sådant som avses i bestämmelserna om till exempel uppvigling, hets mot folkgrupp eller offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen). För att kunna fullgöra sin skyldighet enligt 5 § första stycket lagen om ansvar för elektroniska anslagstavlor ska tillhandahållaren enligt 4 § samma lag ha sådan uppsikt över tjänsten som skäligen kan krävas med hänsyn till omfattningen och inriktningen av verksamheten. Den som uppsåtligen eller av grov oaktsamhet bryter mot 5 § första stycket samma lag kan enligt 7 § första stycket dömas till böter eller fängelse. Något ansvar enligt lagen blir dock inte

aktuellt om det för gärningen kan dömas till ansvar enligt till exempel rekryteringslagen.

Uppdraget att föreslå behörig myndighet

Förordningen kommer att innebära en skyldighet för var och en av medlemsstaterna att utse en eller flera behöriga myndigheter som ska anförtros befogenheter att vidta vissa åtgärder för att förebygga spridning av terrorisminnehåll på internet. En behörig myndighet ska till exempel kunna utfärda en avlägsnandeorder, det vill säga en begäran om att värdtjänstleverantören ska ta bort eller göra visst terrorisminnehåll otillgängligt, och agera för att se till att en värdtjänstleverantör vidtar specifika åtgärder. Medlemsstaterna ska meddela kommissionen vilken eller vilka myndigheter som har utsetts till behörig myndighet senast tolv månader efter att förordningen har trätt i kraft.

Det finns behov av att låta utredaren analysera och föreslå vilken myndighet som ska pekas ut som behörig myndighet för Sveriges räkning enligt förordningen. Endast en myndighet bör vara behörig myndighet eftersom det, för det fall en enda myndighet har samtliga befogenheter till sitt förfogande, skapas bättre förutsättningar för ett effektivt utövande av dem. Mot bakgrund av förordningens innehåll och de krav som förordningen kommer ställa på den behöriga myndigheten bör förslaget avse antingen Polismyndigheten eller Säkerhetspolisen. Det behövs ställningstaganden till vilka författningsändringar och andra åtgärder som krävs för att den föreslagna myndigheten ska kunna tillämpa förordningen och vidta de åtgärder som ankommer på en behörig myndighet enligt förordningen på ett effektivt och rättssäkert sätt. Förslagen ska utformas så att myndighetens administrativa börda inte ökar mer än nödvändigt.

Utredaren ska därför

- ta ställning till om Polismyndigheten eller Säkerhetspolisen bör utses till behörig myndighet enligt förordningen, och
- och lämna nödvändiga författningsförslag.

Uppdraget att föreslå sanktioner och analysera om det i övrigt finns behov att ändra befintlig reglering

Förordningen kommer att kräva att var och en av medlemsstaterna fastställer regler om sanktioner vid värdtjänstleverantörers överträdelser av vissa skyldigheter enligt förordningen och att medlemsstaterna vidtar alla åtgärder som krävs för att säkerställa att dessa regler tillämpas. Medlemsstaterna ska meddela kommissionen vilka regler om sanktioner som gäller senast tolv månader efter att förordningen har trätt i kraft.

Det finns behov av att låta utredaren kartlägga vilka sanktioner som ska kunna följa vid åsidosättanden av aktuella skyldigheter i förordningen. Frågan om det finns behov av att ändra befintlig reglering, däribland dataskyddsregleringen och 5 § första stycket och 7 § lagen om ansvar för elektroniska anslagstavlor bör analyseras, och i förekommande fall bör förslag till författningsändringar tas fram.

Utredaren ska därför

- föreslå vilka sanktioner som ska aktualiseras vid aktuella överträdelser av förordningen,
- analysera i vilken utsträckning förordningen i övrigt medför behov av ändringar eller kompletteringar av svensk rätt, och
- lämna nödvändiga författningsförslag.

Konsekvensbeskrivningar

Utredaren ska analysera och redovisa konsekvenserna av förslagen i enlighet med kommittéförordningen (1998:1474) och förordningen (2007:1244) om konsekvensutredning vid regelgivning. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa förslagens konsekvenser för brottsbekämpningen och säkerställa att förslagen är förenliga med grundläggande fri- och rättigheter. Utredaren ska vidare redovisa förslagens konsekvenser för företagen.

Kontakter och redovisning av uppdraget

I uppdraget ingår inte att lämna förslag till ändring i grundlag. Utredaren ska dock vid sina överväganden noga beakta skyddet för grundläggande fri- och rättigheter, däribland yttrande- och informationsfriheten och förbudet mot dubbelprövning, och se över hur rätten till ett effektivt rättsmedel kan utövas på ett ändamålsenligt sätt enligt vad som kommer att anges i förordningen. Utredarens förslag ska utformas så att företagens totala regelbörda och kostnader inte ökar mer än nödvändigt.

Utredaren får ta upp andra närliggande frågor som har samband med de frågeställningar som ska utredas eller som på annat sätt aktualiseras med anledning av förordningens innehåll om det bedöms nödvändigt.

Under utförandet av uppdraget ska utredaren ha en dialog med och inhämta upplysningar från Polismyndigheten och Säkerhetspolisen. Utredaren ska även, i den utsträckning som bedöms lämpligt, ha en dialog och inhämta upplysningar från andra myndigheter, näringslivet och organisationer som kan vara berörda av aktuella frågor.

Utredaren ska hålla sig informerad om och beakta annat relevant arbete som pågår inom Regeringskansliet och utredningsväsendet samt inom EU och andra internationella forum.

Uppdraget att lämna förslag på behörig myndighet ska redovisas senast den 1 oktober 2021. Uppdraget i övrigt ska redovisas senast den 15 april 2022.

(Justitiedepartementet)

17.5.2021 SV Europeiska unionens officiella tidning L 172/79

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2021/784

av den 29 april 2021

om åtgärder mot spridning av terrorisminnehåll online

(Text av betydelse för EES)

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 [1],

i enlighet med det ordinarie lagstiftningsförfarandet [2], 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 motverka att värdtjänster missbrukas för terrorismändamål samt bidra till den allmänna säkerheten i hela unionen. Den digitala inre marknadens funktion bör förbättras genom att rättssäkerheten ökas för värdtjänstleverantörer och användarnas förtroende för onlinemiljön stärks, samt genom att skyddet för yttrandefriheten förbättras, inbegripet friheten att ta emot och sprida information och idéer i ett öppet och demokratiskt samhälle och mediernas frihet och mångfald.

(2) Regleringsåtgärder för att åtgärda spridningen av terrorisminnehåll online bör kompletteras med strategier från medlemsstaternas sida för att ta itu med terrorism, inbegripet förstärkning av mediekompetens och kritiskt tänkande, utveckling av alternativa budskap och motbudskap samt andra initiativ för att minska effekterna av och mottagligheten för terrorisminnehåll online, liksom investeringar i socialt arbete, avradikaliseringsinitiativ och fördjupade kontakter med berörda samhällsgrupper, för att på ett hållbart sätt förebygga radikalisering i samhället.

(3) Åtgärder mot terrorisminnehåll online, som är en aspekt av ett större problem med olagligt innehåll online, kräver en kombination av lagstiftningsåtgärder, andra åtgärder än lagstiftningsåtgärder samt frivilliga åtgärder som bygger på samarbete mellan myndigheter och värdtjänstleverantörer, på ett sätt som säkerställer fullständig respekt för grundläggande rättigheter.

(4) 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. Värdtjänstleverantörers tjänster missbrukas dock i vissa fall av tredje parter för ändamålet att bedriva olaglig verksamhet online. Särskilt oroande är att terroristgrupper och deras anhängare missbrukar dessa tjänster för att sprida terrorisminnehåll online i syfte att få ut sitt budskap, radikalisera och rekrytera följare samt för att främja och styra terroristverksamhet.

[1] EUT C 110, 22.3.2019, s. 67.
[2] Europaparlamentets ståndpunkt av den 17 april 2019 (ännu inte offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 16 mars 2021 (EUT C 135, 16.4.2021, s. 1). Europaparlamentets ståndpunkt av den 28 april 2021 (ännu inte offentliggjord i EUT).

(5) Även om förekomsten av terrorisminnehåll online inte är den enda faktorn, har den visat sig vara en katalysator för radikalisering av enskilda personer som kan leda till terroristgärningar och får därför allvarliga negativa konsekvenser för användare, medborgare och samhället i stort samt för de leverantörer av onlinetjänster som hyser sådant innehåll, eftersom det undergräver användarnas förtroende och skadar deras affärsmodeller. Med tanke på värdtjänstleverantörernas centrala roll och de tekniska resurser och den tekniska kapacitet som förknippas med de tjänster de tillhandahåller har värdtjänstleverantörerna ett särskilt samhällsansvar att skydda sina tjänster mot missbruk av terrorister och att bidra till att ta itu med terrorisminnehåll som sprids online via deras tjänster, och samtidigt beakta yttrandefrihetens grundläggande betydelse, inbegripet friheten att ta emot och sprida information och idéer i ett öppet och demokratiskt samhälle.

(6) Insatser på unionsnivå för att motverka terrorisminnehåll online inleddes 2015 genom en ram för frivilligt samarbete mellan medlemsstater och värdtjänstleverantörer. Dessa insatser 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 den rättsliga ramen är att bygga vidare på frivilliga insatser, som förstärktes genom kommissionens rekommendation (EU) 2018/334 ([3]), och tillmötesgå uppmaningarna från Europaparlamentet att vidta kraftigare åtgärder mot olagligt och skadligt innehåll online i överensstämmelse med den övergripande ram som inrättades genom Europaparlamentets och rådets direktiv 2000/31/EG ([4]), liksom från Europeiska rådet för att förbättra upptäckten och avlägsnandet av innehåll online som anstiftar till terroristgärningar.

(7) Denna förordning bör inte påverka tillämpningen av direktiv 2000/31/EG. I synnerhet bör inga åtgärder som en värdtjänstleverantör vidtar i enlighet med denna förordning, inbegripet specifika åtgärder, i sig leda till att den värdtjänstleverantören förlorar möjligheten till det undantag från ansvar som föreskrivs i det direktivet. Denna förordning påverkar inte de nationella myndigheternas och domstolarnas befogenheter att fastställa värdtjänstleverantörernas ansvar när villkoren för undantag från ansvar i det direktivet inte är uppfyllda.

(8) Om denna förordning står i konflikt med Europaparlamentets och rådets direktiv 2010/13/EU ([5]) när det gäller bestämmelser om audiovisuella medietjänster enligt definitionen i artikel 1.1 a i det direktivet bör direktiv 2010/13/EU ha företräde. Detta bör inte påverka skyldigheterna enligt denna förordning, i synnerhet vad gäller leverantörer av videodelningsplattformar.

(9) Denna förordning bör fastställa regler som ska motverka att värdtjänster missbrukas för spridning av terrorisminnehåll online i syfte att garantera att den inre marknaden fungerar smidigt. Dessa regler bör fullt ut respektera de grundläggande rättigheter som skyddas i unionen och i synnerhet de som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*).

(10) Syftet med denna förordning är att bidra till att skydda den allmänna säkerheten, samtidigt som lämpliga och stabila skyddsåtgärder fastställs för att säkerställa skyddet av grundläggande rättigheter, inbegripet rätten till respekt för privatlivet, till skydd av personuppgifter, till yttrandefrihet, inklusive friheten att ta emot och sprida information, näringsfriheten samt rätten till ett effektivt rättsmedel. Dessutom är all diskriminering förbjuden. Behöriga myndigheter och värdtjänstleverantörer bör endast anta åtgärder som är nödvändiga, lämpliga och proportionella i ett demokratiskt samhälle, med beaktande av den särskilda vikt som tillmäts yttrande- och informationsfriheten samt mediernas frihet och mångfald, vilka är själva grunden för ett pluralistiskt och demokratiskt samhälle och utgör värden som unionen bygger på. Åtgärder som påverkar yttrande- och informationsfriheten bör vara strikt riktade för att åtgärda spridning av terrorisminnehåll online, samtidigt som rätten att lagligen ta emot och sprida information respekteras, med beaktande av värdtjänstleverantörernas centrala roll i att främja offentlig debatt samt delande och mottagande av fakta, åsikter och idéer, i enlighet med lagen. Effektiva åtgärder online för bekämpning av terrorisminnehåll online och skyddet av yttrande- och informationsfriheten utgör inte motstridiga mål, utan kompletterar och ömsesidigt förstärker varandra.

([3]) 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).

([4]) 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).

([5]) Europaparlamentets och rådets direktiv 2010/13/EU av den 10 mars 2010 om samordning av vissa bestämmelser som fastställs i medlemsstaternas lagar och andra författningar om tillhandahållande av audiovisuella medietjänster (direktiv om audiovisuella mediatjänster) (EUT L 95, 15.4.2010, s. 1).

(11) För att ge klarhet om de åtgärder som både värdtjänstleverantörer och behöriga myndigheter ska vidta för att åtgärda spridningen av terrorisminnehåll online bör denna förordning innehålla en definition av *terrorisminnehåll* i förebyggande syfte, som överensstämmer med definitionerna av relevanta brott i Europaparlamentets och rådets direktiv (EU) 2017/541 ([6]). Med tanke på behovet av att motverka den skadligaste terroristpropagandan online bör den definitionen omfatta material som anstiftar eller värvar någon för att begå eller bidra till att terroristbrott begås, värvar någon för att delta i en terroristgrupps verksamhet, eller förhärligar terroristverksamhet inbegripet genom spridning av material som skildrar en terroristattack. Definitionen bör även omfatta material som ger instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen samt kemiska, biologiska, radiologiska och nukleära (CBRN) ämnen, eller om andra särskilda metoder eller tekniker, inbegripet val av mål i syfte att begå eller bidra till begående av terroristbrott. Sådant material inbegriper text, bilder, ljudupptagningar och videor samt direktsändning av terroristbrott, som innebär en risk för att fler sådana brott begås. Vid bedömningen av huruvida material 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 uttalanden, i vilket sammanhang uttalandena gjordes samt deras potential att få skadliga konsekvenser för människors säkerhet. Det faktum att materialet producerats av, kan tillskrivas eller sprids på uppdrag av en person, grupp eller enhet som ingår i unionens förteckning över personer, grupper och enheter som är delaktiga i terroristgärningar och föremål för restriktiva åtgärder bör utgöra en viktig faktor i bedömningen.

(12) Material som sprids i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller för att öka medvetenheten om terroristverksamhet bör inte anses vara terrorisminnehåll. Vid fastställande av huruvida material som tillhandahålls av en innehållsleverantör utgör *terrorisminnehåll* enligt definitionen i denna förordning bör rätten till yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald samt konstens och vetenskapens frihet särskilt beaktas. I synnerhet i fall där innehållsleverantören har ett redaktionellt ansvar bör varje beslut om avlägsnande av det spridda materialet beakta de publicistiska normer som fastställts genom press- eller mediereglering i enlighet med unionsrätten, inbegripet stadgan. 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.

(13) För att effektivt åtgärda spridningen av terrorisminnehåll online – samtidigt som respekten för enskilda personers privatliv säkerställs – bör denna förordning tillämpas på sådana leverantörer av informationssamhällets tjänster som på begäran lagrar och till allmänheten sprider information och material som tillhandahållits av en användare av tjänsten, oavsett om lagringen och spridningen till allmänheten av sådan information och sådant material är av rent teknisk, automatisk och passiv karaktär. Begreppet *lagring* bör förstås som förvaring av data i minnet hos en fysisk eller virtuell server. Leverantörer av *vidarebefordranstjänster* eller *cachelagringstjänster* samt andra tjänster som tillhandahålls på andra nivåer av internetinfrastrukturen och som inte innefattar lagring, såsom register och registratorer samt leverantörer av domännamnssystem (DNS), betalningstjänster eller skyddstjänster mot samordnad överbelastningsattack (DdoS), bör därför inte omfattas av denna förordnings tillämpningsområde.

(14) Begreppet *spridning till allmänheten* bör innebära att information görs tillgänglig för ett potentiellt obegränsat antal personer, det vill säga att information görs lätt tillgänglig för användare i allmänhet utan att det krävs någon ytterligare åtgärd från innehållsleverantörens sida, oberoende av huruvida dessa personer verkligen tar del av informationen i fråga. Om tillgång till information kräver registrering eller tillträde till en grupp av användare bör den informationen därför anses spridd till allmänheten endast när användare som söker tillgång till informationen automatiskt registreras eller ges tillträde utan att en person beslutar om eller väljer ut vem som ska ges tillgång till informationen. Interpersonella kommunikationstjänster enligt definitionen i artikel 2.5 i Europaparlamentets och rådets direktiv (EU) 2018/1972 ([7]), såsom e-post eller privata meddelandetjänster, bör inte omfattas av denna förordnings tillämpningsområde. Information bör anses lagrad och spridd till allmänheten i den mening

([6]) 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).

([7]) Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

som avses i denna förordning endast när detta sker på direkt begäran av innehållsleverantören. Leverantörer av tjänster, såsom molninfrastruktur, vilka tillhandahålls på begäran av andra parter än innehållsleverantörerna och endast indirekt är till nytta för de sistnämnda, bör därför inte omfattas av denna förordning. Denna förordning bör exempelvis omfatta leverantörer av sociala medietjänster, video-, bild- och ljuddelningstjänster, samt fildelningstjänster och andra molntjänster, i den mån som dessa tjänster används för att göra den lagrade informationen tillgänglig för allmänheten på direkt begäran av innehållsleverantören. Om en värdtjänstleverantör tillhandahåller flera tjänster bör denna förordning endast tillämpas på de tjänster som faller inom dess tillämpningsområde.

(15) Terrorisminnehåll sprids ofta till allmänheten via tjänster som tillhandhålls av värdtjänstleverantörer etablerade i tredjeländer. För att skydda användare i unionen och säkerställa att samtliga värdtjänstleverantörer som verkar inom den digitala inre marknaden omfattas av samma krav bör denna förordning vara tillämplig på alla leverantörer av relevanta tjänster som erbjuds i unionen, oberoende av i vilket land de har sitt huvudsakliga verksamhetsställe. En värdtjänstleverantör bör anses erbjuda tjänster i unionen om den gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster samt har en betydande anknytning till den eller de medlemsstaterna.

(16) En betydande anknytning till unionen bör föreligga om värdtjänstleverantören har ett verksamhetsställe i unionen, om dess tjänster används av ett betydande antal användare i en eller flera medlemsstater, eller om dess verksamhet riktas till en eller flera medlemsstater. Huruvida verksamheten är riktad till en eller flera medlemsstater bör avgöras på grundval av samtliga relevanta omständigheter, inbegripet faktorer som användning av ett språk eller en valuta som i allmänhet används i den berörda medlemsstaten, eller möjligheten att beställa varor eller tjänster från medlemsstaten. En sådan riktad karaktär skulle också kunna härröra från det faktum att en app finns tillgänglig i berörd nationell appstore, att lokal marknadsföring eller reklam görs på ett språk som vanligen används i den berörda medlemsstaten eller att kundkontakter, såsom kundtjänst, sköts på ett språk som vanligen används i den medlemsstaten. En betydande anknytning bör också antas föreligga om en värdtjänstleverantör 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 ([8]). Enbart det faktum att en värdtjänstleverantörs webbplats, en e-postadress eller andra kontaktuppgifter är tillgängliga i en eller flera medlemsstater bör inte i sig vara tillräckligt för att utgöra en betydande anknytning. Dessutom bör det inte kunna anses föreligga en betydande anknytning till unionen på grund av att en tjänst tillhandahålls i det enda syftet att efterleva det förbud mot diskriminering som fastställs i Europaparlamentets och rådets förordning (EU) 2018/302 ([9]).

(17) En harmonisering bör ske av förfarandet för och de skyldigheter som följer av avlägsnandeorder som ålägger värdtjänstleverantörer att avlägsna terrorisminnehåll eller göra det oåtkomligt efter en bedömning av de behöriga myndigheterna. Med tanke på hur snabbt terrorisminnehåll sprids via onlinetjänster bör värdtjänstleverantörerna åläggas en skyldighet att säkerställa att det terrorisminnehåll som anges i avlägsnandeordern avlägsnas eller att det görs oåtkomligt i samtliga medlemsstater inom en timme från mottagandet av avlägsnandeordern. Utom i vederbörligen motiverade brådskande fall bör den behöriga myndigheten tillhandahålla värdtjänstleverantören information om förfaranden och tillämpliga tidsfrister minst tolv timmar innan en avlägsnandeorder för första gången utfärdas till den värdtjänstleverantören. Vederbörligen motiverade brådskande fall föreligger när det faktum att terrorisminnehållet avlägsnas eller görs oåtkomligt senare än en timme efter mottagandet av avlägsnandeordern skulle medföra allvarlig skada, såsom i situationer där det finns ett överhängande hot mot en persons liv eller fysiska integritet eller när sådant innehåll skildrar pågående händelseförlopp som resulterar i skada på en persons liv eller fysiska integritet. Den behöriga myndigheten bör avgöra huruvida enskilda fall utgör brådskande fall och vederbörligen motivera sitt beslut i avlägsnandeordern. Om värdtjänstleverantören på grund av force majeure eller faktisk omöjlighet inte kan följa avlägsnandeordern inom en timme från det att den mottagits, inbegripet på grund av objektivt motiverade tekniska eller operativa skäl, bör den snarast möjligt informera den utfärdande behöriga myndigheten om detta och följa avlägsnandeordern så snart situationen har lösts.

([8]) 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).

([9]) 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 60 I, 2.3.2018, s. 1).

(18) Avlägsnandeordern bör innehålla en motivering som klassificerar det material som ska avlägsnas eller göras oåtkomligt som terrorisminnehåll och ge tillräcklig information för att lokalisera innehållet genom att ange den exakta webbadressen och, när så krävs, eventuell ytterligare information, såsom en skärmdump av innehållet i fråga. Den motiveringen bör göra det möjligt för värdtjänstleverantören och, i slutändan, innehållsleverantören, att faktiskt utöva sin rätt till rättslig prövning. Motiveringen bör inte innebära utlämnande av känslig information som skulle kunna äventyra pågående utredningar.

(19) Den behöriga myndigheten bör lämna avlägsnandeordern direkt till den kontaktpunkt som utsetts eller inrättats av värdtjänstleverantören för tillämpningen av denna förordning, på ett elektroniskt sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar för värdtjänstleverantören att fastställa att ordern är autentisk – även att datum och tidpunkt för sändandet och mottagandet av ordern är korrekta – såsom genom säkrad e-post eller säkrade plattformar eller andra säkra kanaler, även sådana som tillhandahålls av värdtjänstleverantören, i enlighet med unionsrätt om skydd av personuppgifter. Detta krav bör bland annat kunna uppfyllas genom användning av kvalificerade elektroniska tjänster för rekommenderad leverans i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 ([10]). Om värdtjänstleverantören har sitt huvudsakliga verksamhetsställe, eller dess rättsliga företrädare är bosatt eller etablerad, i en annan medlemsstat än den utfärdande behöriga myndighetens medlemsstat bör en kopia av avlägsnandeordern lämnas samtidigt till den behöriga myndigheten i den medlemsstaten.

(20) Den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad bör ha möjlighet att granska den avlägsnandeorder som utfärdats av behöriga myndigheter i en annan medlemsstat för att fastställa huruvida den på ett allvarligt eller uppenbart sätt är oförenlig med denna förordning eller de grundläggande rättigheterna i stadgan. Både innehållsleverantören och värdtjänstleverantören bör ha rätt att begära att den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad ska göra en sådan granskning. När en sådan begäran görs bör den behöriga myndigheten anta ett beslut om huruvida avlägsnandeordern innefattar en sådan oförenlighet. Om en sådan oförenlighet konstateras i det beslutet bör avlägsnandeordern inte längre ha rättsverkan. Granskningen bör utföras snabbt för att säkerställa att innehåll som avlägsnats eller gjorts oåtkomligt på felaktig grund återställs så snart som möjligt.

(21) Värdtjänstleverantörer som är utsatta för terrorisminnehåll och som tillämpar användarvillkor bör i dessa inkludera bestämmelser om åtgärder mot missbruk av deras tjänster för spridning av terrorisminnehåll till allmänheten. De bör tillämpa dessa bestämmelser på ett omsorgsfullt, transparent, proportionellt och icke-diskriminerande sätt.

(22) Med tanke på problemets omfattning och den snabbhet som krävs för att effektivt identifiera och avlägsna terrorisminnehåll är effektiva och proportionella specifika åtgärder en avgörande beståndsdel i kampen mot terrorisminnehåll online. I syfte att minska tillgången till terrorisminnehåll på sina tjänster bör värdtjänstleverantörer som är exponerade för terrorisminnehåll införa specifika åtgärder med beaktande av riskerna för och graden av exponering för terrorisminnehåll samt inverkan på tredje parters rättigheter och allmänhetens intresse av information. Värdtjänstleverantörer bör fastställa vilken lämplig, ändamålsenlig och proportionell specifik åtgärd som bör införas för att identifiera och avlägsna terrorisminnehåll. Specifika åtgärder skulle kunna inbegripa lämpliga tekniska eller operativa åtgärder eller lämplig teknisk eller operativ kapacitet, såsom personal eller tekniska medel för att identifiera och snabbt avlägsna terrorisminnehåll eller göra det oåtkomligt, mekanismer varmed användare kan rapportera eller flagga föregivet terrorisminnehåll, eller varje annan åtgärd som värdtjänstleverantören finner lämplig och effektiv för att åtgärda tillgängligheten av terrorisminnehåll på dess tjänster.

(23) När specifika åtgärder införs bör värdtjänstleverantörerna säkerställa att användares rätt till yttrande- och informationsfrihet samt mediernas frihet och mångfald som skyddas i stadgan bibehålls. Utöver de krav som fastställs i lag, inbegripet lagstiftningen om skydd av personuppgifter, bör värdtjänstleverantörer agera med tillbörlig aktsamhet och vidta skyddsåtgärder, när så är lämpligt, inbegripet mänsklig tillsyn och kontroll, för att undvika oavsiktliga eller felaktiga beslut som leder till att innehåll som inte är terrorisminnehåll avlägsnas eller görs oåtkomligt.

([10]) 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).

(24) Värdtjänstleverantören bör till den behöriga myndigheten rapportera om de specifika åtgärder som införts för att göra det möjligt för den myndigheten att avgöra huruvida åtgärderna är ändamålsenliga och proportionella och, om automatiska metoder används, huruvida värdtjänstleverantören har den nödvändiga kapaciteten för mänsklig tillsyn och kontroll. Vid bedömningen av åtgärdernas ändamålsenlighet och proportionalitet bör de behöriga myndigheterna beakta relevanta parametrar, däribland det antal avlägsnandeorder som utfärdats till värdtjänstleverantören, värdtjänstleverantörens storlek och ekonomiska kapacitet och inverkan av dess tjänster på spridningen av terrorisminnehåll, till exempel på grundval av antalet användare i unionen, samt de skyddsåtgärder som införts för att åtgärda missbruk av dess tjänster för spridning av terrorisminnehåll online.

(25) Om den behöriga myndigheten anser att de specifika åtgärder som införts är otillräckliga för att hantera riskerna bör den kunna kräva att ytterligare lämpliga, ändamålsenliga och proportionella specifika åtgärder antas. Kravet på införande av sådana ytterligare specifika åtgärder bör inte medföra en allmän skyldighet att övervaka eller en skyldighet att aktivt efterforska fakta i den mening som avses i artikel 15.1 i direktiv 2000/31/EG och inte heller något krav på att använda automatiska verktyg. Värdtjänstleverantörer bör emellertid kunna besluta att använda automatiska verktyg om de anser det lämpligt och nödvändigt för att på ett effektivt sätt åtgärda missbruk av deras tjänster för spridning av terrorisminnehåll online.

(26) Värdtjänstleverantörernas skyldighet att bevara avlägsnat innehåll och därtill hörande data bör fastställas för specifika ändamål och begränsas till den tidsperiod som är nödvändig. Det finns ett behov av att utvidga bevarandekravet till därtill hörande data i den mån sådana data annars skulle gå förlorade till följd av att det berörda terrorisminnehållet avlägsnas. Därtill hörande data kan omfatta data såsom abonnentdata, särskilt uppgifter om innehållsleverantörens identitet, och åtkomstdata, inbegripet uppgifter om datum och tidpunkt för innehållsleverantörens användning av och inloggning till och utloggning från tjänsten, tillsammans med den ip-adress som internetleverantören har tilldelat innehållsleverantören.

(27) Skyldigheten att bevara innehållet för administrativa eller rättsliga prövningsförfaranden är nödvändig och motiverad med hänsyn till behovet av att säkerställa att det finns effektiva rättsmedel för innehållsleverantörer vars innehåll har avlägsnats eller gjorts oåtkomligt samt för att säkerställa att innehållet kan återställas beroende på resultatet av dessa förfaranden. Skyldigheten att bevara material för utrednings- eller lagföringsändamål är motiverad och nödvändig med tanke på det värde som materialet kan tillföra för att störa eller förhindra terroristverksamhet. Därför bör bevarande av avlägsnat terrorisminnehåll för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott också anses vara motiverat. Terrorisminnehållet och därtill hörande data bör endast lagras under den tidsperiod som är nödvändig för att de brottsbekämpande myndigheterna ska kunna kontrollera det terrorisminnehållet och besluta om det behövs för dessa ändamål. För förebyggande, förhindrande, upptäckt, utredning och lagföring av terroristbrott bör kravet på att bevara data vara begränsat till data som sannolikt har en koppling till terroristbrott och därmed skulle kunna bidra till att lagföra terroristbrott eller förhindra allvarliga risker för den allmänna säkerheten. När värdtjänstleverantörer avlägsnar material eller gör det oåtkomligt, särskilt genom egna specifika åtgärder, bör de omgående informera de behöriga myndigheterna om innehåll som innehåller information som innefattar ett överhängande hot mot en eller flera personers liv eller ett misstänkt terroristbrott.

(28) För att säkerställa proportionalitet bör perioden för bevarande vara begränsad till sex månader så att innehållsleverantörerna får tillräckligt med tid för att inleda administrativa eller rättsliga prövningsförfaranden och för att brottsbekämpande myndigheter ska kunna få åtkomst till relevanta data för utredning och lagföring av terroristbrott. Det bör dock, på begäran av den behöriga myndigheten eller domstolen, vara möjligt att förlänga denna period med den tid som är nödvändig i fall då dessa förfaranden inleds men inte avslutas inom den sexmånadersperioden. Perioden för bevarande bör vara tillräcklig för att de brottsbekämpande myndigheterna ska kunna bevara material som är nödvändigt för utredningar och lagföring, samtidigt som balansen i förhållande till de grundläggande rättigheterna säkerställs.

(29) Denna förordning bör inte påverka de förfarandegarantier eller processuella utredningsåtgärder som rör åtkomst till innehåll och därtill hörande data som bevarats för att utreda och lagföra terroristbrott, vilka fastställs i unionsrätt eller nationell rätt.

(30) 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 som har vidtagit åtgärder eller ålagts att vidta åtgärder enligt denna förordning under ett visst kalenderår bör offentliggöra årliga transparensrapporter som innehåller information om åtgärder som vidtagits för att identifiera och avlägsna terrorisminnehåll.

(31) De behöriga myndigheterna bör offentliggöra årliga transparensrapporter med information om antalet avlägsnandeorder, antalet fall där en order inte verkställdes, antalet beslut avseende specifika åtgärder, antalet fall som är föremål för administrativa eller rättsliga prövningsförfaranden och antalet beslut om att påföra sanktioner.

(32) Rätten till ett effektivt rättsmedel stadfästs i artikel 19 i fördraget om Europeiska unionen (EU-fördraget) och artikel 47 i stadgan. 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. Den rätten bör särskilt inbegripa en möjlighet för värdtjänstleverantörer och innehållsleverantörer att effektivt bestrida avlägsnandeorder eller beslut till följd av granskning av avlägsnandeorder enligt denna förordning inför domstol i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern eller fattade beslutet, och en möjlighet för värdtjänstleverantörer att effektivt bestrida ett beslut om specifika åtgärder eller sanktioner inför domstol i den medlemsstat vars behöriga myndighet fattade det beslutet.

(33) Klagomålsförfaranden utgör en nödvändig skyddsåtgärd mot att innehåll online felaktigt avlägsnas eller görs oåtkomligt när sådant innehåll är skyddat genom yttrande- 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 innehåll som felaktigt har avlägsnats eller gjorts oåtkomligt bör inte påverka värdtjänstleverantörens möjlighet att genomdriva sina egna användarvillkor.

(34) Ett effektivt rättsligt skydd i enlighet med artikel 19 i EU-fördraget och artikel 47 i stadgan förutsätter att innehållsleverantörer kan utröna av vilka orsaker det innehåll de tillhandahåller har avlägsnats eller gjorts oåtkomligt. För detta ändamål bör värdtjänstleverantören tillhandahålla innehållsleverantören information för bestridande av att innehållet avlägsnats eller gjorts oåtkomligt. Beroende på omständigheterna skulle värdtjänstleverantörer kunna ersätta innehåll som har avlägsnats eller gjorts oåtkomligt med ett meddelande om att innehållet har avlägsnats eller gjorts oåtkomligt i enlighet med denna förordning. Ytterligare information om orsakerna till att innehållet avlägsnats eller gjorts oåtkomligt samt om rättsmedel för detta bör tillhandahållas på begäran från innehållsleverantören. Om de behöriga myndigheterna beslutar att det av hänsyn till allmän säkerhet, inbegripet 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 i enlighet därmed.

(35) Medlemsstaterna bör utse behöriga myndigheter för tillämpningen av denna förordning. Detta bör inte nödvändigtvis innebära att en ny myndighet måste inrättas, och det bör vara möjligt att anförtro ett befintligt organ de funktioner som föreskrivs i denna förordning. Det bör enligt denna förordning finnas krav på att det utses myndigheter som har befogenhet att utfärda avlägsnandeorder, granska avlägsnandeorder, övervaka specifika åtgärder och påföra sanktioner, medan varje medlemsstat bör kunna bestämma hur många behöriga myndigheter som ska utses och om de ska vara administrativa, brottsbekämpande eller rättsliga. Medlemsstaterna bör säkerställa att de behöriga myndigheterna utför sina uppgifter på ett objektivt och icke-diskriminerande sätt och inte efterfrågar eller tar emot instruktioner från något annat organ när det gäller utförandet av uppgifter enligt denna förordning. Detta bör inte förhindra tillsyn i enlighet med nationell konstitutionell rätt. Medlemsstaterna bör underrätta kommissionen om de behöriga myndigheter som utsetts enligt denna förordning, och kommissionen bör offentliggöra ett register online med en förteckning över de behöriga myndigheterna. Det onlineregistret bör vara lätt tillgängligt, så att värdtjänstleverantörer snabbt kan kontrollera att en avlägsnandeorder är autentisk.

(36) För att undvika dubbelarbete och möjlig störning av utredningar samt för att minimera bördan för berörda värdtjänstleverantörer bör de behöriga myndigheterna utbyta information, samordna sig med och samarbeta med varandra och, när så är lämpligt, med Europol, innan de utfärdar avlägsnandeorder. När den fattar beslut om huruvida en avlägsnandeorder ska utfärdas bör den behöriga myndigheten ta vederbörlig hänsyn till eventuella anmälningar om en konflikt med ett utredningsmässigt intresse (konfliktlösning). Om en behörig myndighet får information från en behörig myndighet i en annan medlemsstat om en befintlig avlägsnandeorder bör den inte utfärda en avlägsnandeorder avseende samma sak. Vid genomförandet av bestämmelserna i denna förordning kan Europol tillhandahålla stöd i enlighet med dess nuvarande mandat och befintliga rättsliga ram.

(37) I syfte att säkerställa ett effektivt och tillräckligt enhetligt genomförande av specifika åtgärder som vidtas av värdtjänstleverantörer bör de behöriga myndigheterna samordna sig och samarbeta med varandra i fråga om de utbyten som de har med värdtjänstleverantörer avseende avlägsnandeorder samt identifiering, genomförande och bedömning av specifika åtgärder. Samordning och samarbete behövs också i samband med andra åtgärder för genomförande av denna förordning, inbegripet med avseende på antagande av regler om sanktioner och påförande av sanktioner. Kommissionen bör underlätta sådan samordning och sådant samarbete.

(38) Det är viktigt att den behöriga myndigheten i den medlemsstat som ansvarar för att påföra sanktioner är fullständigt informerad om utfärdandet av avlägsnandeorder och efterföljande utbyten mellan värdtjänstleverantören och behöriga myndigheter i andra medlemsstater. För det ändamålet bör medlemsstaterna säkerställa lämpliga och säkra kommunikationskanaler och mekanismer som gör det möjligt att dela relevant information i rätt tid.

(39) För att underlätta ett snabbt utbyte mellan behöriga myndigheter och med värdtjänstleverantörer, och för att undvika dubbelarbete, bör medlemsstaterna uppmuntras att använda sig av de särskilda verktyg som utvecklats av Europol, såsom den befintliga applikationen för hantering av anmälan av innehåll på internet (*Internet Referral Management application*) eller dess efterföljare.

(40) Anmälningar från medlemsstaterna och Europol har visat sig utgöra ett effektivt och snabbt sätt att öka värdtjänstleverantörers medvetenhet om specifikt innehåll som är tillgängligt via deras tjänster och göra det möjligt för dem att snabbt vidta åtgärder. Sådana anmälningar, som är en mekanism för att uppmärksamma värdtjänstleverantörer på information som skulle kunna anses utgöra terrorisminnehåll, så att de frivilligt kan bedöma om det innehållet är förenligt med deras egna användarvillkor, bör förbli tillgängliga vid sidan av avlägsnandeorder. Det är alltjämt värdtjänstleverantören som fattar det slutliga beslutet om huruvida innehållet ska avlägsnas på grund av att det är oförenligt med dess användarvillkor. Denna förordning bör inte påverka Europols mandat som fastställs i Europaparlamentets och rådets förordning (EU) 2016/794 ([11]). Ingenting i den här förordningen bör därför tolkas som att det skulle hindra medlemsstaterna och Europol från att använda anmälningar som ett verktyg för åtgärdande av terrorisminnehåll online.

(41) Med tanke på de särskilt allvarliga konsekvenserna av visst terrorisminnehåll online bör värdtjänstleverantörer omgående informera de relevanta myndigheterna i den berörda medlemsstaten eller de behöriga myndigheterna i den medlemsstat där de är etablerade eller har en rättslig företrädare om terrorisminnehåll som innefattar ett överhängande hot mot en eller flera personers liv eller ett misstänkt terroristbrott. För att säkerställa proportionalitet bör den skyldigheten vara begränsad till terroristbrott enligt definitionen i artikel 3.1 i direktiv (EU) 2017/541. Den skyldigheten att informera bör inte innebära att värdtjänstleverantörer är skyldiga att aktivt söka bevis på sådana överhängande hot mot en eller flera personers liv eller ett misstänkt terroristbrott. Den berörda medlemsstaten bör förstås som den medlemsstat som har jurisdiktion över utredning och lagföring av de terroristbrotten på grundval av gärningsmannens eller det potentiella brottsoffrets nationalitet eller målplatsen för terroristgärningen. Om det råder tvivel bör värdtjänstleverantörer lämna informationen till Europol som bör tillhandahålla relevanta uppföljningsåtgärder i enlighet med sitt mandat, inbegripet genom att vidarebefordra den informationen till de relevanta nationella myndigheterna. Medlemsstaternas behöriga myndigheter bör ha rätt att använda sådan information för att vidta utredningsåtgärder som föreskrivs i unionsrätt eller nationell rätt.

([11]) 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).

(42) Värdtjänstleverantörer bör utse eller inrätta kontaktpunkter för att underlätta snabb handläggning av avlägsnandeorder. Kontaktpunkten bör endast tjäna operativa syften. Kontaktpunkten bör bestå av någon typ av särskilda medel, interna eller externa, som möjliggör elektronisk inlämning av avlägsnandeorder och av tekniska resurser eller personalresurser som möjliggör snabb handläggning av dem. Kontaktpunkten måste inte vara belägen i unionen. Värdtjänstleverantören bör vara fri att använda en befintlig kontaktpunkt vid tillämpningen av denna förordning, under förutsättning att kontaktpunkten 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 kontaktpunkten för värdtjänstleverantörer som är exponerade för terrorisminnehåll vara tillgänglig vid alla tidpunkter. 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 unionsinstitutionernas officiella språk som deras användarvillkor finns tillgängliga på.

(43) Då det inte finns något allmänt krav på att värdtjänstleverantörer måste säkerställa fysisk närvaro inom 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 dess huvudsakliga verksamhetsställe är beläget eller där dess rättsliga företrädare är bosatt eller etablerad. Detta bör inte påverka de bestämmelser om behörighet som fastställs för avlägsnandeorder och beslut som följer av granskningen av avlägsnandeorder enligt denna förordning. När det gäller en värdtjänstleverantör som inte har något verksamhetsställe i unionen och som inte utser en rättslig företrädare bör varje medlemsstat ändå ha jurisdiktion och därmed kunna påföra sanktioner, under förutsättning att principen *ne bis in idem* respekteras.

(44) Värdtjänstleverantörer som inte är etablerade i unionen bör skriftligen utse en rättslig företrädare för att säkerställa att skyldigheterna enligt denna förordning efterlevs och verkställs. Värdtjänstleverantörer bör för tillämpningen av denna förordning kunna utse en rättslig företrädare som redan är utsedd för andra ändamål, under förutsättning att denna rättsliga företrädare kan fullgöra de funktioner som föreskrivs i denna förordning. Den rättsliga företrädaren bör ha befogenhet att agera på värdtjänstleverantörens vägnar.

(45) Sanktioner är nödvändiga för att säkerställa värdtjänstleverantörernas effektiva genomförande av denna förordning. Medlemsstaterna bör anta regler om sanktioner, som kan vara av administrativ eller straffrättslig art, samt riktlinjer för bötfällning när så är lämpligt. Bristande efterlevnad i enskilda fall kan bli föremål för sanktioner, med respekt för principen *ne bis in idem* och proportionalitetsprincipen, samt med säkerställande av att sådana sanktioner påförs med beaktande av systematisk underlåtenhet. Sanktioner kan ta sig olika former, inbegripet formella varningar vid smärre överträdelser eller böter vid allvarligare eller systematiska överträdelser. Särskilt stränga sanktioner bör fastställas om värdtjänstleverantören systematiskt eller fortgående underlåter att avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme från mottagandet av en avlägsnandeorder. För att säkerställa rättssäkerhet bör det i denna förordning anges vilka överträdelser som kan bli föremål för sanktioner och vilka omständigheter som är relevanta för att bedöma sanktionernas typ och nivå. Vid fastställande av huruvida böter ska åläggas bör vederbörlig hänsyn tas till värdtjänstleverantörens ekonomiska resurser. Den behöriga myndigheten bör vidare ta hänsyn till huruvida värdtjänstleverantören är ett nystartat företag eller ett mikroföretag, litet eller medelstort företag enligt definitionen i kommissionens rekommendation 2003/361/EG ([12]). Ytterligare omständigheter bör beaktas, exempelvis huruvida värdtjänstleverantörens handlande objektivt sett varit oförsiktigt eller klandervärt eller huruvida överträdelsen har orsakats av vårdslöshet eller varit avsiktlig. Medlemsstaterna bör säkerställa att de sanktioner som påförs för överträdelser av denna förordning inte uppmuntrar till avlägsnande av material som inte är terrorisminnehåll.

(46) Användningen av standardiserade mallar underlättar samarbete och informationsutbyte mellan behöriga myndigheter och värdtjänstleverantörer, 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. Mallar minskar översättningskostnaderna och bidrar till en högre standard för processen. Mallar för återkoppling möjliggör ett standardiserat informationsutbyte och är särskilt viktiga om värdtjänstleverantörerna inte kan följa avlägsnandeorder. Autentiserade inlämningskanaler kan garantera att avlägsnandeordern är autentisk, liksom att datum och tidpunkt för sändande och mottagande av ordern är korrekta.

([12]) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

(47) För att vid behov möjliggöra en snabb ändring 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 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, inbegripet på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([13]). 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.

(48) Medlemsstaterna bör samla in information om genomförandet av denna förordning. Medlemsstaterna bör ha möjlighet att använda sig av värdtjänstleverantörernas transparensrapporter och vid behov komplettera med mer detaljerad information, såsom deras egna transparensrapporter enligt denna förordning. Ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter bör inrättas som underlag för en utvärdering av genomförandet av denna förordning.

(49) På grundval av resultaten och slutsatserna i genomföranderapporten och resultaten av övervakningen bör kommissionen genomföra en utvärdering av denna förordning inom tre år från dagen för dess ikraftträdande. Utvärderingen bör grundas på kriterierna effektivitet, nödvändighet, ändamålsenlighet, proportionalitet, relevans, samstämmighet och mervärde för unionen. Den bör inkludera en bedömning av hur de olika operativa och tekniska åtgärder som föreskrivs i denna förordning fungerar, inbegripet ändamålsenligheten i de åtgärder som ska förbättra upptäckt, identifiering och avlägsnande av terrorisminnehåll online, skyddsmekanismernas ändamålsenlighet samt inverkan på grundläggande rättigheter som potentiellt påverkas, såsom yttrande- och informationsfriheten, inbegripet mediernas frihet och mångfald, näringsfriheten, rätten till ett privatliv och skyddet av personuppgifter. Kommissionen bör även bedöma inverkan på tredje parters potentiellt påverkade intressen.

(50) Eftersom målet för denna förordning, nämligen att säkerställa att den digitala inre marknaden fungerar smidigt genom åtgärder mot spridningen av terrorisminnehåll online, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av dess omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. 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

Innehåll och tillämpningsområde

1. I denna förordning fastställs enhetliga regler för att åtgärda missbruk av värdtjänster för spridning till allmänheten av terrorisminnehåll online, i synnerhet följande:

a) Rimliga och proportionella aktsamhetskrav som värdtjänstleverantörer ska iaktta för att åtgärda spridning till allmänheten av terrorisminnehåll via deras tjänster och vid behov säkerställa att sådant innehåll snabbt avlägsnas eller görs oåtkomligt.

([13]) EUT L 123, 12.5.2016, s. 1.

b) Åtgärder som medlemsstaterna ska införa – i enlighet med unionsrätten och med förbehåll för lämpliga skyddsåtgärder för att skydda grundläggande rättigheter, särskilt yttrande- och informationsfriheten i ett öppet och demokratiskt samhälle – för att

i) identifiera och göra det möjligt för värdtjänstleverantörer att snabbt avlägsna terrorisminnehåll, samt

ii) underlätta samarbete mellan medlemsstaternas behöriga myndigheter, värdtjänstleverantörer och, när så är lämpligt, Europol.

2. Denna förordning är tillämplig på värdtjänstleverantörer som erbjuder tjänster i unionen, oberoende av deras huvudsakliga verksamhetsställe, i den mån de sprider information till allmänheten.

3. Material som sprids till allmänheten i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller i syfte att förhindra eller bekämpa terrorism, inbegripet material som ger uttryck för polemiska eller kontroversiella åsikter inom ramen för den offentliga debatten, ska inte anses vara terrorisminnehåll. Det ska göras en bedömning för att fastställa den spridningens verkliga syfte och huruvida materialet sprids till allmänheten för dessa syften.

4. Denna förordning ska inte medföra någon ändring av skyldigheten att respektera de rättigheter, friheter och principer som avses i artikel 6 i EU-fördraget och ska tillämpas utan att det påverkar tillämpningen av grundläggande principer som rör yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald.

5. Denna förordning ska inte påverka tillämpningen av direktiven 2000/31/EG och 2010/13/EU. För audiovisuella medietjänster enligt definitionen i artikel 1.1 a i direktiv 2010/13/EU ska direktiv 2010/13/EU äga företräde.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *värdtjänstleverantör*: en leverantör av tjänster enligt definitionen i artikel 1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([14]) som består i att information som tillhandahållits av en innehållsleverantör lagras på dennes begäran.

2. *innehållsleverantör*: en användare som har tillhandahållit information som lagras och sprids till allmänheten eller har lagrats och spridits till allmänheten av en värdtjänstleverantör.

3. *spridning till allmänheten*: tillgängliggörande av information på begäran av en innehållsleverantör för ett potentiellt obegränsat antal personer.

4. *erbjuda tjänster i unionen*: göra det möjligt för fysiska eller juridiska 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.

5. *betydande anknytning*: en värdtjänstleverantörs anknytning till en eller flera medlemsstater som antingen följer av dennes verksamhetsställe i unionen eller särskilda faktiska kriterier, såsom att

a) värdtjänstleverantören har ett betydande antal användare av dess tjänster i en eller flera medlemsstater, eller

b) värdtjänstleverantörens verksamhet är riktad till en eller flera medlemsstater.

6. *terroristbrott*: brott enligt definitionen i artikel 3 i direktiv (EU) 2017/541.

([14]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

7. *terrorisminnehåll*: en eller flera av följande typer av material, närmare bestämt material som

a) anstiftar till begåendet av ett av de brott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541, om sådant material, direkt eller indirekt, såsom genom förhärligande av terroristgärningar, förespråkar begåendet av terroristbrott, och därigenom medför fara för att ett eller flera sådana brott kan begås,

b) värvar en person eller en grupp av personer för att begå något av de brott som anges i artikel 3.1 a–i i direktiv (EU) 2017/541 eller bidra till att något av dessa brott begås,

c) värvar en person eller en grupp av personer för att delta i en terroristgrupps verksamhet i den mening som avses i artikel 4 b i direktiv (EU) 2017/541,

d) tillhandahåller instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen eller om andra specifika metoder eller tekniker för begående av eller bidragande till begåendet av något av de terroristbrott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541,

e) utgör ett hot om begående av ett av de brott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541.

8. *användarvillkor*: alla krav, villkor och klausuler som, oberoende av deras namn eller form, reglerar avtalsförhållandet mellan en värdtjänstleverantör och dess användare.

9. *huvudsakligt verksamhetsställe*: värdtjänstleverantörens huvudkontor eller säte, där de huvudsakliga finansiella funktionerna och den operativa ledningen utövas.

AVSNITT II

ÅTGÄRDER MOT SPRIDNING AV TERRORISMINNEHÅLL ONLINE

Artikel 3

Avlägsnandeorder

1. Den behöriga myndigheten i varje medlemsstat ska ha befogenhet att utfärda en avlägsnandeorder med krav på att värdtjänstleverantörer avlägsnar terrorisminnehåll eller gör terrorisminnehåll oåtkomligt i samtliga medlemsstater.

2. Om en behörig myndighet inte tidigare har utfärdat en avlägsnandeorder till en värdtjänstleverantör ska den tillhandahålla den värdtjänstleverantören information om tillämpliga förfaranden och tidsfrister minst tolv timmar innan avlägsnandeordern utfärdas.

Första stycket ska inte gälla i vederbörligen motiverade brådskande fall.

3. Värdtjänstleverantörer ska avlägsna terrorisminnehåll eller göra terrorisminnehåll oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern.

4. Behöriga myndigheter ska utfärda avlägsnandeorder med användning av mallen i bilaga I. Avlägsnandeorder ska innehålla följande uppgifter:

a) Identifieringsuppgifter för den behöriga myndighet som utfärdar avlägsnandeordern och den behöriga myndighetens autentisering av avlägsnandeordern.

b) En tillräckligt detaljerad motivering till varför innehållet anses utgöra terrorisminnehåll samt en hänvisning till den relevanta typen av material enligt artikel 2.7.

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

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

e) Datum, tidsstämpel och elektronisk signatur för den behöriga myndighet som utfärdar avlägsnandeordern.

f) Lättbegriplig information om värdtjänstleverantörens och innehållsleverantörens prövningsmöjligheter, inbegripet information om prövning vid såväl den behöriga myndigheten som vid domstol samt tidsfrister för överklagande.

g) När så är nödvändigt och proportionellt, beslutet att inte lämna ut information om att terrorisminnehåll avlägsnats eller gjorts oåtkomligt i enlighet med artikel 11.3.

5. Den behöriga myndigheten ska rikta avlägsnandeordern till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till dess rättsliga företrädare som utsetts i enlighet med artikel 17.

Den behöriga myndigheten ska överföra avlägsnandeordern till den kontaktpunkt som avses i artikel 15.1 på ett elektroniskt sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar att säkerställa autentisering av avsändaren, inbegripet att datum och tidpunkt för sändandet och mottagandet av ordern är korrekta.

6. Värdtjänstleverantören ska utan onödigt dröjsmål med användning av mallen i bilaga II informera den behöriga myndigheten om att terrorisminnehållet har avlägsnats eller att terrorisminnehållet gjorts oåtkomligt i samtliga medlemsstater, med angivelse av i synnerhet tidpunkten då innehållet avlägsnades eller gjordes oåtkomligt.

7. Om värdtjänstleverantören inte kan följa avlägsnandeordern på grund av force majeure eller faktisk omöjlighet som inte kan tillskrivas värdtjänstleverantören, inbegripet av objektivt motiverade tekniska eller operativa skäl, ska den utan onödigt dröjsmål informera den behöriga myndighet som utfärdade avlägsnandeordern om dessa skäl med användning av mallen i bilaga III.

Den tidsfrist som anges i punkt 3 ska börja löpa så snart de grunder som avses i första stycket i denna punkt inte längre föreligger.

8. Om värdtjänstleverantören inte kan följa avlägsnandeordern på grund av att den innehåller uppenbara fel eller inte innehåller tillräcklig information för att verkställa den, ska värdtjänstleverantören utan onödigt dröjsmål informera den behöriga myndighet som utfärdade avlägsnandeordern och be om nödvändiga klargöranden med användning av mallen i bilaga III.

Den tidsfrist som anges i punkt 3 ska börja löpa så snart värdtjänstleverantören har mottagit de nödvändiga klargörandena.

9. En avlägsnandeorder ska bli slutgiltig vid utgången av tidsfristen för överklagande om inget överklagande har ingetts i enlighet med nationell rätt eller vid bekräftelse efter ett överklagande.

När avlägsnandeordern har blivit slutgiltig ska den behöriga myndighet som utfärdade avlägsnandeordern informera den behöriga myndighet som avses i artikel 12.1 c i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad om detta.

Artikel 4

Förfarande för gränsöverskridande avlägsnandeorder

1. Med förbehåll för vad som anges i artikel 3 ska den behöriga myndighet som utfärdade avlägsnandeordern, om värdtjänstleverantören inte har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i den medlemsstat där den myndigheten är belägen, samtidigt översända en kopia av avlägsnandeordern till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad.

2. Om en värdtjänstleverantör mottar en avlägsnandeorder enligt denna artikel ska den vidta de åtgärder som föreskrivs i artikel 3 och vidta de åtgärder som krävs för att kunna återställa innehållet eller åtkomsten till det i enlighet med punkt 7 i den här artikeln.

3. Den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad får på eget initiativ, inom 72 timmar från mottagandet av kopian av avlägsnandeordern i enlighet med punkt 1, granska avlägsnandeorden för att fastställa huruvida den på ett allvarligt eller uppenbart sätt är oförenlig med denna förordning eller de grundläggande rättigheter och friheter som garanteras i stadgan.

Om den konstaterar oförenlighet ska den, inom samma tid, anta ett motiverat beslut om detta.

4. Värdtjänstleverantörer och innehållsleverantörer ska ha rätt att inom 48 timmar från mottagandet av antingen en avlägsnandeorder eller information enligt artikel 11.2 lämna in en motiverad begäran till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad om att den ska granska avlägsnandeordern enligt punkt 3 första stycket i den här artikeln.

Den behöriga myndigheten ska inom 72 timmar från mottagandet av begäran anta ett motiverat beslut till följd av granskningen av avlägsnandeordern, med angivande av sina slutsatser om huruvida oförenlighet föreligger.

5. Innan den behöriga myndigheten antar ett beslut enligt punkt 3 andra stycket eller ett beslut om att oförenlighet föreligger enligt punkt 4 andra stycket ska den informera den behöriga myndighet som utfärdat avlägsnandeordern om att den har för avsikt anta beslutet i fråga samt ange skälen till detta.

6. Om den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad antar ett motiverat beslut i enlighet med punkt 3 eller 4 i denna artikel, ska den utan dröjsmål översända det beslutet till den behöriga myndighet som utfärdat avlägsnandeordern, värdtjänstleverantören, den innehållsleverantör som begärde granskningen enligt punkt 4 i denna artikel samt, i enlighet med artikel 14, Europol. Om det i beslutet konstateras oförenlighet enligt punkt 3 eller 4 i denna artikel, ska avlägsnandeordern inte längre ha rättsverkan.

7. När den berörda värdtjänstleverantören mottar ett beslut i vilket oförenlighet konstateras som översänts i enlighet med punkt 6 ska den omedelbart återställa det avlägsnade innehållet eller åtkomsten till det utan att det påverkar dess möjlighet att genomdriva sina egna användarvillkor i enlighet med unionsrätten och nationell rätt.

Artikel 5

Specifika åtgärder

1. En värdtjänstleverantör som är exponerad för terrorisminnehåll enligt punkt 4 ska i tillämpliga fall i sina användarvillkor inkludera samt tillämpa bestämmelser om åtgärder mot missbruk av dess tjänster för spridning till allmänheten av terrorisminnehåll.

Den ska göra detta på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt och under alla omständigheter med vederbörlig hänsyn till användarnas grundläggande rättigheter och med särskilt beaktande av den grundläggande betydelsen av yttrande- och informationsfrihet i ett öppet och demokratiskt samhälle, i syfte att undvika avlägsnandet av material som inte är terrorisminnehåll.

2. En värdtjänstleverantör som är exponerad för terrorisminnehåll enligt punkt 4 ska vidta specifika åtgärder för att skydda sina tjänster mot spridning till allmänheten av terrorisminnehåll.

Det är värdtjänstleverantören som ska besluta vilka specifika åtgärder som ska vidtas. Sådana åtgärder får inbegripa en eller flera av följande åtgärder:

a) Lämpliga tekniska och operativa åtgärder eller lämplig teknisk och operativ kapacitet, såsom lämplig personalstyrka eller lämpliga tekniska medel för att identifiera och snabbt avlägsna terrorisminnehåll eller göra det oåtkomligt.

b) Lättillgängliga och användarvänliga mekanismer varmed användare till värdtjänstleverantören kan rapportera eller flagga påstått terrorisminnehåll.

c) Andra mekanismer för att öka medvetenheten om terrorisminnehåll på dess tjänster, såsom mekanismer för användarmoderering.

d) Andra åtgärder som värdtjänstleverantören anser vara lämpliga för att åtgärda tillgängligheten av terrorisminnehåll på dess tjänster.

3. Specifika åtgärder ska uppfylla samtliga följande krav:

a) De ska på ett effektivt sätt minska graden av exponering för terrorisminnehåll hos värdtjänstleverantörens tjänster.

b) De ska vara riktade och proportionella, med särskilt beaktande av hur hög graden av exponering för terrorisminnehåll är hos värdtjänstleverantörens tjänster samt värdtjänstleverantörens tekniska och operativa kapacitet och finansiella styrka samt antalet användare av värdtjänstleverantörens tjänster och den mängd innehåll som de tillhandahåller.

c) De ska tillämpas med fullständigt beaktande av användarnas rättigheter och legitima intressen, särskilt användarnas grundläggande rättigheter vad gäller yttrande- och informationsfrihet, respekt för privatlivet samt skydd av personuppgifter.

d) De ska tillämpas på ett omsorgsfullt och icke-diskriminerande sätt.

När de specifika åtgärderna innebär användning av tekniska medel ska det införas lämpliga och effektiva skyddsåtgärder, särskilt genom mänsklig tillsyn och kontroll, för att säkerställa att de är korrekta och för att undvika avlägsnande av material som inte är terrorisminnehåll.

4. En värdtjänstleverantör är exponerad för terrorisminnehåll när den behöriga myndigheten i den medlemsstat där den har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad har

a) fattat ett beslut som grundas på objektiva faktorer, såsom det faktum att värdtjänstleverantören under de föregående tolv månaderna har mottagit två eller flera avlägsnandeorder som blivit slutgiltiga, i vilket det konstateras att värdtjänstleverantören är exponerad för terrorisminnehåll, och

b) meddelat värdtjänstleverantören det beslut som avses i led a.

5. Efter att ha mottagit ett beslut som avses i punkt 4 eller, i förekommande fall, punkt 6 ska en värdtjänstleverantör till den behöriga myndigheten rapportera om de specifika åtgärder som den har vidtagit och har för avsikt att vidta för att följa punkterna 2 och 3. Den ska göra detta inom tre månader från mottagandet av beslutet och därefter årligen. Denna skyldighet ska upphöra så snart den behöriga myndigheten har beslutat, till följd av en begäran enligt punkt 7, att värdtjänstleverantören inte längre är exponerad för terrorisminnehåll.

6. Om den behöriga myndigheten – på grundval av de rapporter som avses i punkt 5 och i förekommande fall andra objektiva faktorer – anser att de specifika åtgärder som vidtagits inte uppfyller kraven i punkterna 2 och 3, ska den behöriga myndigheten rikta ett beslut till värdtjänstleverantören med krav på att denne vidtar nödvändiga åtgärder för att säkerställa att kraven i punkterna 2 och 3 uppfylls.

Värdtjänstleverantören får välja vilken typ av specifika åtgärder som ska vidtas.

7. En värdtjänstleverantör får när som helst begära att den behöriga myndigheten omprövar och, när så är lämpligt, ändrar eller återkallar ett beslut som avses i punkt 4 eller 6.

Inom tre månader från mottagandet av begäran ska den behöriga myndigheten på grundval av objektiva faktorer anta ett motiverat beslut om begäran samt meddela värdtjänstleverantören det beslutet.

8. Krav på att vidta specifika åtgärder ska inte påverka tillämpningen av artikel 15.1 i direktiv 2000/31/EG och ska varken medföra en allmän skyldighet för värdtjänstleverantörer att övervaka den information som de överför eller lagrar eller en allmän skyldighet att aktivt efterforska fakta eller omständigheter som tyder på olaglig verksamhet.

Inget krav på att vidta specifika åtgärder får innebära en skyldighet för värdtjänstleverantören att använda automatiska verktyg.

Artikel 6

Bevarande av innehåll och därtill hörande data

1. Värdtjänstleverantörer ska bevara terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder, eller specifika åtgärder enligt artikel 3 eller 5, samt därtill hörande data som har avlägsnats till följd av att sådant terrorisminnehåll har avlägsnats, som är nödvändiga för

a) administrativa eller rättsliga prövningsförfaranden eller hantering av klagomål enligt artikel 10 avseende ett beslut att avlägsna eller göra oåtkomligt terrorisminnehåll och därtill hörande data,

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

2. Det terrorisminnehåll och de därtill hörande data som avses i punkt 1 ska bevaras i sex månader från det att de avlägsnats eller gjorts oåtkomliga. Terrorisminnehållet ska på den behöriga myndighetens eller domstolens begäran bevaras under en ytterligare, specificerad period endast 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 därtill hörande data som bevaras enligt punkt 1 omfattas av lämpliga tekniska och organisatoriska skyddsåtgärder.

Dessa tekniska och organisatoriska skyddsåtgärder ska säkerställa att det terrorisminnehåll och de därtill hörande 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 7

Transparenskrav för värdtjänstleverantörer

1. Värdtjänstleverantörer ska i sina användarvillkor klart och tydligt ange sin strategi för att åtgärda spridningen av terrorisminnehåll, när så är lämpligt med en meningsfull förklaring av hur specifika åtgärder, inbegripet i förekommande fall användningen av automatiska verktyg, fungerar.

2. Varje värdtjänstleverantör som har vidtagit åtgärder för att åtgärda spridningen av terrorisminnehåll eller har ålagts att vidta åtgärder enligt denna förordning under ett visst kalenderår ska offentliggöra en transparensrapport om dessa åtgärder för det året. Den ska offentliggöra den rapporten före den 1 mars följande år.

3. Transparensrapporterna ska innehålla minst följande information:

a) Information om värdtjänstleverantörens åtgärder för att identifiera och avlägsna terrorisminnehåll eller göra det oåtkomligt.

b) Information om värdtjänstleverantörens åtgärder för att åtgärda att material som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det ansågs vara terrorisminnehåll dyker upp på nytt, särskilt när automatiska verktyg har använts.

c) Antalet inslag med terrorisminnehåll som har avlägsnats eller gjorts oåtkomliga till följd av avlägsnandeorder eller specifika åtgärder samt antalet avlägsnandeorder där innehållet inte har avlägsnats eller gjorts oåtkomligt enligt artikel 3.7 första stycket och 3.8 första stycket tillsammans med skälen till detta.

d) Antalet klagomål som behandlats av värdtjänstleverantören i enlighet med artikel 10 och resultatet av dessa.

e) Antalet administrativa eller rättsliga prövningsförfaranden som inletts av värdtjänstleverantören och resultatet av dessa.

f) Antalet fall där värdtjänstleverantören har ålagts att återställa innehåll eller åtkomsten till det till följd av administrativa eller rättsliga prövningsförfaranden.

g) Antalet fall där värdtjänstleverantören har återställt innehåll eller åtkomsten till det till följd av ett klagomål från innehållsleverantören.

Artikel 8

Behöriga myndigheters transparensrapporter

1. De behöriga myndigheterna ska offentliggöra årliga transparensrapporter över sin verksamhet enligt denna förordning. Dessa rapporter ska innehålla åtminstone följande information för kalenderåret i fråga:

a) Antalet avlägsnandeorder som har utfärdats enligt artikel 3, med angivande av antalet avlägsnandeorder enligt artikel 4.1, och det antal avlägsnandeorder som granskats enligt artikel 4 samt information om hur de berörda värdtjänstleverantörerna har genomfört dessa avlägsnandeorder, inbegripet antalet fall där terrorisminnehåll har avlägsnats eller gjorts oåtkomligt och antalet fall där terrorisminnehåll inte har avlägsnats eller gjorts oåtkomligt.

b) Antalet beslut som fattats i enlighet med artikel 5.4, 5.6 eller 5.7 samt information om hur värdtjänstleverantörerna har genomfört dessa beslut, inbegripet en beskrivning av de specifika åtgärderna.

c) Antalet fall där avlägsnandeorder och beslut som fattats i enlighet med artikel 5.4 och 5.6 har varit föremål för administrativa eller rättsliga prövningsförfaranden samt information om resultatet av de relevanta förfarandena.

d) Antalet beslut om påförande av sanktioner enligt artikel 18 och en beskrivning av den typ av sanktion som påförts.

2. De årliga transparensrapporter som avses i punkt 1 får inte innehålla information som negativt kan påverka pågående verksamhet för förebyggande, förhindrande, upptäckt, utredning eller lagföring av terroristbrott eller nationella säkerhetsintressen.

Artikel 9

Rättsmedel

1. Värdtjänstleverantörer som har mottagit en avlägsnandeorder som utfärdats enligt artikel 3.1 eller ett beslut enligt artikel 4.4 eller artikel 5.4, 5.6 eller 5.7 ska ha rätt till ett effektivt rättsmedel. Denna rätt ska inbegripa rätten att bestrida en sådan avlägsnandeorder inför domstolarna i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern och rätten att bestrida beslutet enligt artikel 4.4 eller artikel 5.4, 5.6 eller 5.7 inför domstolarna i den medlemsstat vars behöriga myndighet fattade beslutet.

2. Innehållsleverantörer vars innehåll har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder ska ha rätt till ett effektivt rättsmedel. Denna rätt ska inbegripa rätten att bestrida en avlägsnandeorder som har utfärdats enligt artikel 3.1 inför domstolarna i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern och rätten att bestrida ett beslut enligt artikel 4.4 inför domstolarna i den medlemsstat vars behöriga myndighet fattade beslutet.

3. Medlemsstaterna ska införa effektiva förfaranden för utövandet av de rättigheter som avses i denna artikel.

Artikel 10

Klagomålsmekanismer

1. Varje värdtjänstleverantör ska inrätta en effektiv och tillgänglig mekanism som gör det möjligt för innehållsleverantörer att, när deras innehåll har avlägsnats eller gjorts oåtkomligt till följd av specifika åtgärder enligt artikel 5, lämna in ett klagomål mot att innehållet avlägsnats eller gjorts oåtkomligt med en begäran om att det avlägsnade innehållet eller åtkomsten till det återställs.

2. Varje värdtjänstleverantör ska snabbt granska alla klagomål som den tar emot genom den mekanism som avses i punkt 1 och utan onödigt dröjsmål återställa innehållet eller åtkomsten till det om det inte var berättigat att avlägsna innehållet eller göra det oåtkomligt. Den ska informera klaganden om resultatet av klagomålet inom två veckor från det att det mottagits.

Om klagomålet avslås ska värdtjänstleverantören underrätta klaganden om skälen till dess beslut.

Ett återställande av innehåll eller åtkomsten till det ska inte utesluta administrativa eller rättsliga prövningsförfaranden för bestridande av värdtjänstleverantörens eller den behöriga myndighetens beslut.

Artikel 11

Information till innehållsleverantörer

1. Om en värdtjänstleverantör avlägsnar terrorisminnehåll eller gör det oåtkomligt ska den ge innehållsleverantören information om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

2. På innehållsleverantörens begäran ska värdtjänstleverantören antingen informera innehållsleverantören om skälen till att innehållet avlägsnades eller gjordes oåtkomligt och dess rätt att bestrida avlägsnandeordern eller tillhandahålla innehållsleverantören en kopia av avlägsnandeordern.

3. Skyldigheten enligt punkterna 1 och 2 ska inte gälla om den behöriga myndighet som utfärdar avlägsnandeordern beslutar att det är nödvändigt och proportionellt att skälen inte lämnas ut av hänsyn till allmän säkerhet, såsom förebyggande, förhindrande, utredning, upptäckt och lagföring av terroristbrott, under så lång tid som det är nödvändigt, men inte längre än sex veckor efter det beslutet. I ett sådant fall ska värdtjänstleverantören inte lämna någon information om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

Den behöriga myndigheten får förlänga den perioden med ytterligare sex veckor, om det fortfarande finns motiverade skäl till att inte lämna ut skälen.

AVSNITT IV

BEHÖRIGA MYNDIGHETER OCH SAMARBETE

Artikel 12

Utseende av behöriga myndigheter

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

a) utfärda avlägsnandeorder enligt artikel 3,

b) granska avlägsnandeorder enligt artikel 4,

c) övervaka genomförandet av specifika åtgärder enligt artikel 5,

d) påföra sanktioner enligt artikel 18.

2. Varje medlemsstat ska säkerställa att en kontaktpunkt utses eller inrättas inom den behöriga myndighet som avses i punkt 1 a för att hantera begäranden om klargöranden och återkoppling avseende avlägsnandeorder som har utfärdats av den behöriga myndigheten.

Medlemsstaterna ska säkerställa att information om kontaktpunkten offentliggörs.

3. Senast den 7 juni 2022 ska medlemsstaterna underrätta kommissionen om den eller de behöriga myndigheter som avses i punkt 1 och eventuella ändringar avseende dessa. Kommissionen ska offentliggöra underrättelsen och eventuella ändringar därav i *Europeiska unionens officiella tidning*.

4. Senast den 7 juni 2022 ska kommissionen upprätta ett onlineregister med en förteckning över de behöriga myndigheter som avses i punkt 1 och den kontaktpunkt som utsetts eller inrättats enligt punkt 2 för varje behörig myndighet. Kommissionen ska regelbundet offentliggöra eventuella ändringar avseende dessa.

Artikel 13

Behöriga myndigheter

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

2. Medlemsstaterna ska säkerställa att deras behöriga myndigheter utför sina uppgifter enligt denna förordning på ett objektivt och icke-diskriminerande sätt med fullständig respekt för grundläggande rättigheter. De behöriga myndigheterna får inte efterfråga eller ta emot instruktioner från något annat organ när det gäller utförandet av uppgifter enligt artikel 12.1.

Första stycket ska inte förhindra tillsyn i enlighet med nationell konstitutionell rätt.

Artikel 14

Samarbete mellan värdtjänstleverantörer, behöriga myndigheter och Europol

1. De behöriga myndigheterna ska utbyta information, samordna sig med och samarbeta med varandra och, när så är lämpligt, med Europol, avseende avlägsnandeorder, i synnerhet för att undvika dubbelarbete, förbättra samordningen och undvika att störa utredningar i andra medlemsstater.

2. Medlemsstaternas behöriga myndigheter ska utbyta information, samordna sig med och samarbeta med de behöriga myndigheter som avses i artikel 12.1 c och d avseende specifika åtgärder som vidtas enligt artikel 5 och sanktioner som påförs enligt artikel 18. Medlemsstaterna ska säkerställa att de behöriga myndigheter som avses i artikel 12.1 c och d förfogar över all relevant information.

3. Vid tillämpningen av punkt 1 ska medlemsstaterna sörja för lämpliga och säkra kommunikationskanaler eller mekanismer för att säkerställa att den relevanta informationen utbyts i rätt tid.

4. För en effektiv tillämpning av denna förordning och för att undvika dubbelarbete får medlemsstater och värdtjänstleverantörer använda särskilda verktyg, inbegripet sådana som inrättats av Europol, för att särskilt underlätta

a) handläggning och återkoppling avseende avlägsnandeorder enligt artikel 3, och

b) samarbete i syfte att identifiera och genomföra specifika åtgärder enligt artikel 5.

5. Om värdtjänstleverantörer får kännedom om terrorisminnehåll som medför ett överhängande hot mot en eller flera personers liv ska de omgående underrätta de myndigheter som är behöriga att utreda och lagföra brott i de berörda medlemsstaterna. Om det är omöjligt att identifiera de berörda medlemsstaterna ska värdtjänstleverantörerna underrätta kontaktpunkten enligt artikel 12.2 i den medlemsstat där de har sitt huvudsakliga verksamhetsställe eller där deras rättsliga företrädare är bosatt eller etablerad och vidarebefordra information om det terrorisminnehållet till Europol för lämplig uppföljning.

6. De behöriga myndigheterna uppmanas att skicka kopior av avlägsnandeorder till Europol så att Europol kan tillhandahålla en årlig rapport med en analys av vilka typer av terrorisminnehåll som har varit föremål för en avlägsnandeorder eller en order om att göra det oåtkomligt enligt denna förordning.

Artikel 15

Värdtjänstleverantörers kontaktpunkter

1. Varje värdtjänstleverantör ska utse eller inrätta en kontaktpunkt för mottagande av avlägsnandeorder på elektronisk väg och snabb handläggning av dem enligt artiklarna 3 och 4. Värdtjänstleverantören ska säkerställa att information om kontaktpunkten offentliggörs.

2. I den information som avses i punkt 1 i denna artikel ska det anges på vilka av unionsinstitutionernas officiella språk som avses i förordning 1/58 ([15]) som kontaktpunkten kan kontaktas och ytterligare utbyten avseende avlägsnandeorder enligt artikel 3 ska äga rum. Dessa språk ska omfatta åtminstone ett av de officiella språken i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad.

AVSNITT V

GENOMFÖRANDE OCH VERKSTÄLLIGHET

Artikel 16

Jurisdiktion

1. Den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe ska ha jurisdiktion vid tillämpningen av artiklarna 5, 18 och 21. En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen ska anses lyda under jurisdiktionen i den medlemsstat där dess rättsliga företrädare är bosatt eller etablerad.

2. Om en värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen inte har utsett en rättslig företrädare ska samtliga medlemsstater ha jurisdiktion.

3. Om en behörig myndighet i en medlemsstat utövar jurisdiktion enligt punkt 2 ska den informera de behöriga myndigheterna i alla övriga medlemsstater.

Artikel 17

Rättslig företrädare

1. En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen ska skriftligen utse en fysisk eller juridisk person till sin rättsliga företrädare i unionen för mottagande, efterlevnad och verkställighet av avlägsnandeorder och beslut som utfärdas av de behöriga myndigheterna.

2. Värdtjänstleverantören ska förse sin rättsliga företrädare med de befogenheter och resurser som krävs för att följa dessa avlägsnandeorder och beslut och för att samarbeta med de behöriga myndigheterna.

Den rättsliga företrädaren ska vara bosatt eller etablerad i en av de medlemsstater där värdtjänstleverantören erbjuder sina tjänster.

3. Den rättsliga företrädaren får hållas ansvarig för överträdelser av denna förordning, utan att det påverkar värdtjänstleverantörens eventuella ansvarighet eller eventuella rättsliga åtgärder mot denne.

4. Värdtjänstleverantören ska underrätta den behöriga myndighet som avses i artikel 12.1 d i den medlemsstat där dess rättsliga företrädare är bosatt eller etablerad om utseendet.

Informationen om den rättsliga företrädaren ska offentliggöras av värdtjänstleverantören.

AVSNITT VI

SLUTBESTÄMMELSER

Artikel 18

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för värdtjänstleverantörers överträdelser av bestämmelserna i denna förordning och vidta alla åtgärder som krävs för att säkerställa att de tillämpas. Sådana sanktioner ska vara begränsade till överträdelser av artiklarna 3.3 och 3.6, 4.2 och 4.7, 5.1, 5.2, 5.3, 5.5 och 5.6, 6, 7, 10 och 11, 14.5, 15.1 och 17.

([15]) Förordning nr 1 om vilka språk som skall användas i Europeiska ekonomiska gemenskapen (EGT 17, 6.10.1958, s. 385).

De sanktioner som avses i första stycket ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 7 juni 2022 samt utan dröjsmål eventuella ändringar som berör dem.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de beslutar huruvida en sanktion ska påföras och när de fastställer sanktioneras typ och nivå, beaktar alla relevanta omständigheter, inbegripet

a) överträdelsens karaktär, allvar och varaktighet,

b) om överträdelsen var avsiktlig eller orsakades av vårdslöshet,

c) tidigare överträdelser som värdtjänstleverantören har gjort sig skyldig till,

d) värdtjänstleverantörens finansiella styrka,

e) graden av tjänsteleverantörens samarbete med de behöriga myndigheterna,

f) värdtjänstleverantörens karaktär och storlek, i synnerhet huruvida det är ett mikroföretag, litet eller medelstort företag,

g) graden av skuld hos värdtjänstleverantören, med beaktande av de tekniska och organisatoriska åtgärder som den har vidtagit för att följa denna förordning.

3. Medlemsstaterna ska säkerställa att en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3 blir föremål för böter på upp till 4 % av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret.

Artikel 19

Tekniska krav och ändringar av bilagorna

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

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 20 för att ändra bilagorna i syfte att effektivt åtgärda eventuella behov av förbättringar av innehållet i mallarna för avlägsnandeorder och för att meddela att det är omöjligt att verkställa avlägsnandeorder.

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 ges till kommissionen tills vidare från och med den 7 juni 2022.

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 av den 13 april 2016 om bättre lagstiftning.

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 värdtjänstleverantörer under deras jurisdiktion om de åtgärder som dessa under det föregående kalenderåret har vidtagit i enlighet med denna förordning och sända informationen till kommissionen senast den 31 mars varje år. Denna information ska omfatta följande:

a) Antalet utfärdade avlägsnandeorder och antalet inslag med terrorisminnehåll som har avlägsnats eller gjorts oåtkomliga, och hur fort de har avlägsnats eller gjorts oåtkomliga.

b) De specifika åtgärder som har vidtagits enligt artikel 5, inklusive antalet inslag med terrorisminnehåll som har avlägsnats eller gjorts oåtkomliga, och hur fort de har avlägsnats eller gjorts oåtkomliga.

c) Antalet begäranden om åtkomst som har utfärdats av behöriga myndigheter avseende innehåll som bevaras av värdtjänstleverantörer enligt artikel 6.

d) Antalet klagomålsförfaranden som har inletts och de åtgärder som vidtagits av värdtjänstleverantörerna enligt artikel 10.

e) Antalet administrativa eller rättsliga prövningsförfaranden som har inletts och beslut som fattats av den behöriga myndigheten i enlighet med nationell rätt.

2. Senast den 7 juni 2023 ska kommissionen inrätta ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter. I övervakningsprogrammet ska de indikatorer och metoder som ska användas för att samla in uppgifter och andra nödvändiga belägg anges samt med vilka intervaller insamlingen 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 enligt artikel 23.

Artikel 22

Genomföranderapport

Senast den 7 juni 2023 ska kommissionen lägga fram en rapport för Europaparlamentet och rådet om tillämpningen av denna förordning. Den rapporten ska inkludera information om övervakning enligt artikel 21 och information som härrör från transparenskraven enligt artikel 8. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta rapporten.

Artikel 23

Utvärdering

Senast den 7 juni 2024 ska kommissionen göra en utvärdering av denna förordning och lägga fram en rapport för Europaparlamentet och rådet om dess tillämpning, inklusive

a) funktionen hos och ändamålsenligheten i skyddsmekanismerna, särskilt de som föreskrivs i artiklarna 4.4, 6.3 och 7–11,

b) den inverkan som tillämpningen av denna förordning har på de grundläggande rättigheterna, särskilt yttrande- och informationsfriheten, respekten för privatlivet och skyddet av personuppgifter, samt

c) denna förordnings bidrag till att skydda den allmänna säkerheten.

Vid behov ska rapporten åtföljas av lagstiftningsförslag.

Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta rapporten.

Kommissionen ska även bedöma hur nödvändigt och genomförbart det är att inrätta en europeisk plattform om terrorisminnehåll online för att underlätta kommunikation och samarbete enligt denna förordning.

Artikel 24

Ikraftträdande och tillämpning

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 7 juni 2022.

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

Utfärdad i Bryssel den 29 april 2021.

På Europaparlamentets vägnar	*På rådets vägnar*
D.M. SASSOLI	A.P. ZACARIAS
Ordförande	*Ordförande*

BILAGA I

AVLÄGSNANDEORDER

(artikel 3 i Europaparlamentets och rådets förordning (EU) 2021/784)

Enligt artikel 3 i förordning (EU) 2021/784 (*förordningen*) ska den som mottar denna avlägsnandeorder avlägsna terrorisminnehåll eller göra terrorisminnehåll oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern.

Enligt artikel 6 i förordningen ska mottagaren bevara innehåll och därtill hörande data som har avlägsnats eller gjorts oåtkomliga i sex månader eller längre på begäran av behöriga myndigheter eller domstolar.

Enligt artikel 15.2 i förordningen ska denna avlägsnandeorder sändas på ett av de språk som mottagaren har angett.

AVSNITT A:

Den utfärdande behöriga myndighetens medlemsstat:

.....

Anm.: uppgifter om den utfärdande behöriga myndigheten ska lämnas i avsnitten E och F

Mottagare och, om tillämpligt, rättslig företrädare:

.....

Kontaktpunkt:

.....

Medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad:

.....

Tid och datum för utfärdande av avlägsnandeordern:

.....

Referensnummer för avlägsnandeordern:

.....

AVSNITT B: Terrorisminnehåll som ska avlägsnas eller göras oåtkomligt i alla medlemsstater så snart som möjligt och i alla händelser inom en timme efter mottagandet av avlägsnandeordern:

Webbadress (URL) och eventuell annan information som gör det möjligt att identifiera och hitta exakt plats för terrorisminnehållet:

.....

Orsaker till att materialet anses vara terrorisminnehåll, i enlighet med artikel 2.7 i förordningen.

Materialet (kryssa för relevant(a) ruta/rutor)

☐ anstiftar andra till att begå terroristbrott, exempelvis genom att förhärliga terroristgärningar, genom att förespråka att sådana brott begås (artikel 2.7 a i förordningen)

☐ värvar andra för att begå eller bidra till begåendet av terroristbrott (artikel 2.7 b i förordningen)

☐ värvar andra för att delta i en terroristgrupps verksamhet (artikel 2.7 c i förordningen)

☐ tillhandahåller instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen, eller om andra specifika metoder eller tekniker för begående av eller bidragande till begående av terroristbrott (artikel 2.7 d i förordningen)

☐ utgör ett hot om begående av ett av terroristbrotten (artikel 2.7 e i förordningen)

Ytterligare information om orsakerna till att materialet anses vara terrorisminnehåll:

.....

.....

.....

AVSNITT C: Information till innehållsleverantören

Observera att (kryssa för rutan, om det är tillämpligt)

☐ mottagaren **får** av hänsyn till allmän säkerhet **inte informera innehållsleverantören** om att innehållet avlägsnas eller görs oåtkomligt

Om rutan inte är tillämplig, se avsnitt G för uppgifter om möjligheterna enligt nationell rätt att bestrida avlägsnandeordern i den utfärdande behöriga myndighetens medlemsstat (en kopia av avlägsnandeordern måste på begäran skickas till innehållsleverantören).

AVSNITT D: Information till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad

Kryssa för relevant(a) ruta/rutor

☐ Den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad är en annan än den utfärdande behöriga myndighetens medlemsstat

☐ En kopia av avlägsnandeordern skickas till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad

AVSNITT E: Uppgifter om den utfärdande behöriga myndigheten

Typ (kryssa för relevant ruta)

☐ domare, domstol eller undersökningsdomare

☐ brottsbekämpande myndighet

☐ annan behörig myndighet → fyll även i avsnitt F

Uppgifter om den utfärdande behöriga myndigheten eller dess företrädare, som intygar att avlägsnandeordern är riktig och korrekt

Den utfärdande behöriga myndighetens namn:

.....

Namn på myndighetens företrädare och dennes befattning (titel och grad):

.....

Dokumentnummer:

.....

Adress:

.....

Tfn (landsnummer) (riktnummer):

.....

Fax (landsnummer) (riktnummer):

.....

E-postadress .....

Datum.....

Officiell stämpel (om tillämpligt) och underskrift [1]:

.....

[1] En underskrift är inte nödvändig om avlägsnandeordern sänds via autentiserade inlämningskanaler som kan garantera att avlägsnandeordern är autentisk.

AVSNITT F: Kontaktuppgifter för uppföljning

Kontaktuppgifter till den utfärdande behöriga myndigheten för återkoppling om den tidpunkt då innehållet nades eller gjordes oåtkomligt, eller för att lämna ytterligare klargöranden:

.....

Kontaktuppgifter till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvu verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad:

.....

AVSNITT G: Information om möjligheter till prövning

Information om behörigt organ eller behörig domstol, tidsfrister och förfaranden för bestridande av avlägsn dern

Behörigt organ eller behörig domstol vid vilken avlägsnandeordern kan bestridas:

.....

Tidsfrist för bestridande av avlägsnandeordern (dagar/månader från och med):

.....

Länk till bestämmelser i nationell lagstiftning:

.....

BILAGA II

ÅTERKOPPLING EFTER DET ATT TERRORISMINNEHÅLL HAR AVLÄGSNATS ELLER GJORTS OÅTKOMLIGT

(artikel 3.6 i Europaparlamentets och rådets förordning (EU) 2021/784)

AVSNITT A:

Avlägsnandeorderns mottagare:

.....

Behörig myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för den behöriga myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för mottagaren:

.....

Tid och datum för mottagande av avlägsnandeordern:

.....

AVSNITT B: Åtgärder som vidtagits i enlighet med avlägsnandeordern

(Kryssa för relevant ruta)

☐ terrorisminnehållet har avlägsnats

☐ terrorisminnehållet har gjorts oåtkomligt i alla medlemsstater

Tid och datum då åtgärden vidtogs:

.....

AVSNITT C: Uppgifter om mottagaren

Namn på värdtjänstleverantören:

.....

ELLER

Namn på värdtjänstleverantörens rättsliga företrädare:

.....

Medlemsstat där värdtjänstleverantörens har sitt huvudsakliga verksamhetsställe:

.....

ELLER

Medlemsstat där värdtjänstleverantörens rättsliga företrädare är bosatt eller etablerad:

.....

Namn på den bemyndigade personen:

.....

Kontaktpunktens e-postadress:

.....

Datum:

.....

BILAGA III

INFORMATION OM ATT DET ÄR OMÖJLIGT ATT VERKSTÄLLA AVLÄGSNANDEORDERN

(artikel 3.7 och 3.8 i Europaparlamentets och rådets förordning (EU) 2021/784)

AVSNITT A:

Avlägsnandeorderns mottagare:

.....

Behörig myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för den behöriga myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för mottagaren:

.....

Tid och datum för mottagande av avlägsnandeordern:

.....

AVSNITT B: Utebliven verkställighet

1. Avlägsnandeordern kan inte verkställas inom tidsfristen av följande orsaker (kryssa för relevant(a) ruta/rutor):

☐ force majeure eller faktisk omöjlighet som inte kan tillskrivas värdtjänstleverantören, inbegripet av objektivt motiverade tekniska eller operativa skäl

☐ avlägsnandeordern innehåller uppenbara fel

☐ avlägsnandeordern innehåller inte tillräckligt med information

2. Redogör närmare för orsakerna till utebliven verkställighet:

.....

3. Om avlägsnandeordern innehåller uppenbara fel och/eller inte innehåller tillräckligt med information, precisera felen och den ytterligare information eller de ytterligare klargöranden som krävs:

.....

AVSNITT C: Uppgifter om värdtjänstleverantören eller dess rättsliga företrädare

Namn på värdtjänstleverantören:

.....

ELLER

Namn på värdtjänstleverantörens rättsliga företrädare:

.....

Namn på den bemyndigade personen:

.....

Kontaktuppgifter (e-postadress):

.....

Underskrift:

.....

Tid och datum:

.....

Statens offentliga utredningar 2021

Kronologisk förteckning

1. Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. I.
2. Krav på kunskaper i svenska och samhällskunskap för svenskt medborgarskap. Ju.
3. Skolbibliotek för bildning och utbildning. U.
4. Informationsöverföring inom vård och omsorg. S.
5. Ett förbättrat system för arbetskraftsinvandring. Ju.
6. God och nära vård. Rätt stöd till psykisk hälsa. S.
7. Förstärkt skydd för väljarna vid röstmottagningen. Ju.
8. När behovet får styra – ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). S.
9. Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen. I.
10. Radiologiska skador – skadestånd, säkerheter, skadereglering. M.
11. Bättre möjligheter för elever att nå kunskapskraven – aktivt stöd- och elevhälsoarbete samt stärkt utbildning för elever med intellektuell funktionsnedsättning. U.
12. Andra chans för krisande företag – En ny lag om företagsrekonstruktion. Ju.
13. En teknikneutral grundlagsbestämmelse för regeringsbeslut. Ju.
14. Boende på (o)lika villkor – merkostnader i bostad med särskild service för vuxna enligt LSS. S.
15. Föreningsfrihet och terroristorganisationer. Ju.
16. En väl fungerande ordning för val och beslutsfattande i kommuner och regioner. Fi.
17. Ett moderniserat konsumentskydd. Fi.
18. Bolags rörlighet över gränserna. Volym 1 & 2. Ju.
19. En stärkt försörjningsberedskap för hälso- och sjukvården. Del 1 och 2. S.
20. Ecris-TCN – ett mer effektivt utbyte av brottmålsdomar mot tredjelandsmedborgare. Ju.
21. En klimatanpassad miljöbalk för samtiden och framtiden. M.
22. Hårdare regler för nya nikotinprodukter. S.
23. Stärkt planering för en hållbar utveckling. Fi.
24. Äga avfall – en del av den cirkulära ekonomin. M.
25. Struktur för ökad motståndskraft. Ju.
26. Använd det som fungerar. M.
27. Ett förbud mot rasistiska organisationer. Ju.
28. Immunitet för utställningsföremål. Ku.
29. Ökade möjligheter att förhindra illegal handel via post. I.
30. Kampen om tiden – mer tid till lärande. U.
31. Kontroller på väg. I.
32. Papper, poddar och ... Pliktmateriallagstiftning för ett tryggat källmaterial. U.
33. En tioårig grundskola. Införandet av en ny årskurs 1 i grundskolan, grundsärskolan, specialskolan och sameskolan. U.
34. Börja med barnen! En sammanhållen god och nära vård för barn och unga. S.
35. En stärkt rättsprocess och en ökad lagföring. Ju.

36. Gode män och förvaltare – en översyn. Ju.
37. Stärkt rätt till personlig assistans. Ökad rättssäkerhet för barn, fler grundläggande behov och tryggare sjukvårdande insatser. S.
38. En ny lag om ordningsvakter m.m. Ju.
39. Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården. S.
40. Mervärdesskatt vid inhyrd personal för vård och social omsorg. Fi.
41. VAB för vårdåtgärder i skolan. S.
42. Stärkta åtgärder mot penningtvätt och finansiering av terrorism. Fi.
43. Ett förstärkt skydd mot sexuella kränkningar. Ju.
44. Tillgänglighetsdirektivet. S.
45. En EU-anpassad djurläkemedelslagstiftning. Del 1 och 2. N.
46. Snabbare lagföring – ett snabbförfarande i brottmål. Ju.
47. Ett nytt regelverk för bygglov. Del 1 och 2. Fi.
48. I en värld som ställer om. Sverige utan fossila drivmedel 2040. M.
49. Kommuner mot brott. Ju.
50. Fri hyressättning vid nyproduktion. Ju.
51. Skydd av arter – vårt gemensamma ansvar. Vol. 1 och 2. M.
52. Vilja välja vård och omsorg. En hållbar kompetensförsörjning inom vård och omsorg om äldre. S.
53. En rättssäker vindkraftsprövning. M.
54. Ändrade regler i medborgarskapslagen. Ju.
55. Mikroföretagarkonto – schabloniserad inkomstbeskattning för de minsta företagen. Fi.
56. Nya regler om utländska föräldraskap och adoption i vissa fall. Ju.
57. Om folkbokföring, samordningsnummer och identitetsnummer. Fi.
58. Läge och kvalitet i hyressättningen. Ju.
59. Vägen till tillgänglighet – långsiktig, strategisk och i samverkan. S.
60. Förenklingar för mikroföretag och modernisering av bokföringslagen. N.
61. Utvisning på grund av brott – ett skärpt regelverk. Ju.
62. Användning av e-legitimation i tjänsten i den offentliga förvaltningen. I.
63. Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem. Fö.
64. Ersättning till brottsoffer. Ju.
65. Stärkt fokus på framtidens forskningsinfrastruktur. U.
66. Rätt mottagare. Demokrativillkor och integritet. Ku.
67. Vägen mot fossiloberoende jordbruk. N.
68. Skärpta straff för brott i kriminella nätverk. Ju.
69. En sjukförsäkring med prevention, rehabilitering och trygghet. Volym 1 och 2. S.
70. Läromedelsutredningen – böckernas betydelse och elevernas tillgång till kunskap. U.
71. Riksintressen i hälso- och sjukvården – stärkt statlig styrning för hållbar vårdinfrastruktur. S.
72. Högskoleprovets organisation och styrning. U.
73. Regler för statliga elvägar. I.
74. Ett modernt belöningssystem, de allmänna flaggdagarna och redovisningen av anslaget till hovet. Ju.
75. En god kommunal hushållning. + Digital bilagedel för bilaga 3–6. Fi.
76. EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet. Ju.

Statens offentliga utredningar 2021

Systematisk förteckning

Ersättning till brottsoffer. [64]

Skärpta straff för brott i kriminella nätverk. [68]

Ett modernt belöningssystem, de allmänna flaggdagarna och redovisningen av anslaget till hovet. [74]

EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet. [76]

Kulturdepartementet

Immunitet för utställningsföremål. [28]

Rätt mottagare. Demokrativillkor och integritet. [66]

Miljödepartementet

Radiologiska skador – skadestånd, säkerheter, skadereglering. [10]

En klimatanpassad miljöbalk för samtiden och framtiden. [21]

Äga avfall – en del av den cirkulära ekonomin. [24]

Använd det som fungerar. [26]

I en värld som ställer om. Sverige utan fossila drivmedel 2040. [48]

Skydd av arter – vårt gemensamma ansvar. Vol. 1 och 2. [51]

En rättssäker vindkraftsprövning. [53]

Näringsdepartementet

En EU-anpassad djurläkemedelslagstiftning. Del 1 och 2. [45]

Förenklingar för mikroföretag och modernisering av bokföringslagen. [60]

Vägen mot fossiloberoende jordbruk. [67]

Socialdepartementet

Informationsöverföring inom vård och omsorg. [4]

God och nära vård. Rätt stöd till psykisk hälsa. [6]

När behovet får styra – ett tandvårdssystem för en mer jämlik tandhälsa. Vol. 1 & Vol. 2, bilagor + Sammanfattning (häfte). [8]

Boende på (o)lika villkor – merkostnader i bostad med särskild service för vuxna enligt LSS. [14]

En stärkt försörjningsberedskap för hälso- och sjukvården. Del 1 och 2. [19]

Hårdare regler för nya nikotinprodukter. [22]

Börja med barnen! En sammanhållen god och nära vård för barn och unga. [34]

Stärkt rätt till personlig assistans. Ökad rättssäkerhet för barn, fler grundläggande behov och tryggare sjukvårdande insatser. [37]

Ombuds tillgång till vård- och omsorgsuppgifter och förenklad behörighetskontroll inom vården. [39]

VAB för vårdåtgärder i skolan. [41]

Tillgänglighetsdirektivet. [44]

Vilja välja vård och omsorg. En hållbar kompetensförsörjning inom vård och omsorg om äldre. [52]

Vägen till ökad tillgänglighet – långsiktig, strategisk och i samverkan. [59]

En sjukförsäkring med prevention, rehabilitering och trygghet. Volym 1 och 2. [69]

Riksintressen i hälso- och sjukvården – stärkt statlig styrning för hållbar vårdinfrastruktur. [71]

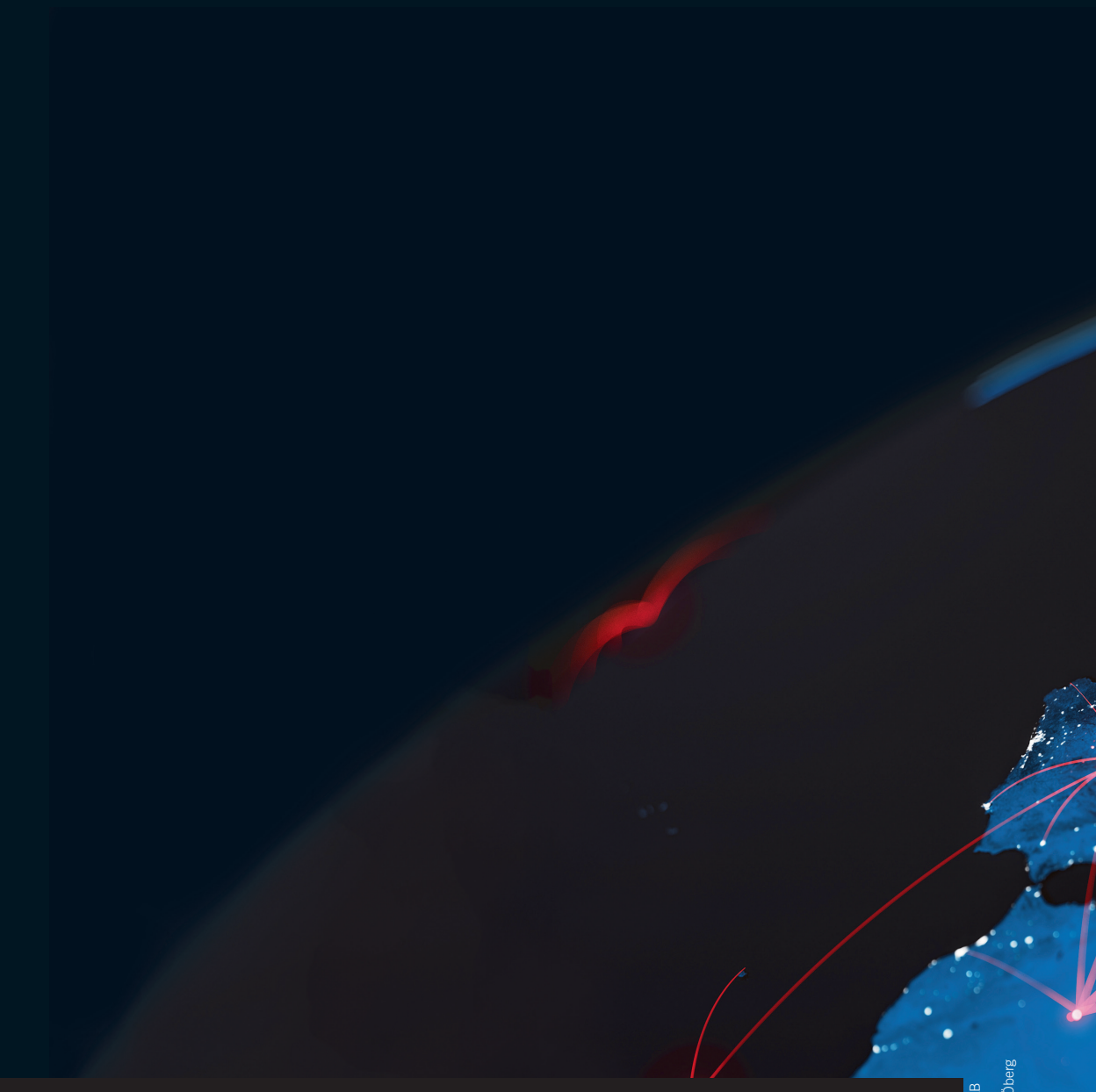
Utbildningsdepartementet

Skolbibliotek för bildning och utbildning. [3]

Bättre möjligheter för elever att nå kunskapskraven – aktivt stöd- och elevhälsoarbete samt stärkt utbildning för elever med intellektuell funktionsnedsättning. [11]

Kampen om tiden – mer tid till lärande. [30]

Papper, poddar och ... Pliktmateriallagstiftning för ett tryggat källmaterial. [32]



Regeringskansliet

103 33 Stockholm Växel 08-405 10 00 www.regeringen.se

ISBN 978-91-525-0216-7 ISSN 0375-250X

Omslag: Elanders Sverige AB
Bild: maginima
Bildbearbetning: Agneta S Öberg