

Lagrådsremiss

Effektivare åtgärder mot spridning av terrorisminnehåll online

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 19 januari 2023

Gunnar Strömmer

Johan Stensbäck
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Sedan den 7 juni 2022 tillämpas EU:s förordning om åtgärder mot spridning av terrorisminnehåll online. Förordningen ger de nationella behöriga myndigheterna vissa befogenheter och ålägger s.k. värdtjänstleverantörer vissa skyldigheter. Bland annat får den behöriga myndigheten utfärda order om att en värdtjänstleverantör ska avlägsna terrorisminnehåll från sin värdtjänst, vilket denne är skyldig att göra inom en timme från mottagandet av en sådan order.

För att uppfylla kraven i EU-förordningen och möjliggöra en effektiv tillämpning av den föreslår regeringen bland annat en ny lag som ger Polismyndigheten, som är behörig myndighet i Sverige, möjlighet att besluta om vitesförelägganden och sanktionsavgifter mot värdtjänstleverantörer. Lagen möjliggör även nödvändigt uppgiftsutbyte mellan Polismyndigheten och Säkerhetspolisen.

Den nya lagen och övriga lagändringar föreslås träda i kraft den 1 juli 2023.

Innehållsförteckning

1	Beslut	4
2	Lagtext	5
2.1	Förslag till lag med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online	5
2.2	Förslag till lag om ändring i lagen (1998:112) om ansvar för elektroniska anslagstavlor	7
2.3	Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)	8
2.4	Förslag till lag om ändring i radio- och tv-lagen (2010:696)	9
3	Ärendet och dess beredning	10
4	TCO-förordningens syfte och huvudsakliga innehåll	10
5	En ny lag som kompletterar TCO-förordningen	14
5.1	En ny lag med bestämmelser som kompletterar TCO-förordningen ska införas	14
5.2	En bestämmelse om behörig myndighet	15
6	Förhållandet till yttrande- och informationsfrihet	16
6.1	Skyddet för yttrande- och informationsfrihet	16
6.2	TCO-förordningens förhållande till skyddet för yttrande- och informationsfrihet	19
7	Sanktioner	22
7.1	TCO-förordningens krav på sanktioner	22
7.2	TCO-förordningens krav bör uppfyllas genom bestämmelser om administrativa sanktioner	22
7.3	Vitesförelägganden	24
7.3.1	Den behöriga myndigheten ska kunna besluta om vitesföreläggande	24
7.3.2	Handläggningen av ärenden om vitesföreläggande	26
7.3.3	Vitesbeloppet	26
7.4	Sanktionsavgifter	27
7.4.1	Den behöriga myndigheten ska kunna besluta om sanktionsavgift	27
7.4.2	Sanktionsavgiftens storlek	29
7.4.3	Förfarandet vid beslut om sanktionsavgift	30
7.5	Särskilt om förbudet mot dubbelbestraffning	31
8	Sekretess, uppgiftsutbyte och dataskydd	32
8.1	Sekretess hos Polismyndigheten	32
8.2	En ny bestämmelse om uppgiftsskyldighet	35
8.3	Informationsutbyte mellan medlemsstaternas behöriga myndigheter	37
8.4	Förhållandet till dataskyddsregleringen	38

9	Rätten att överklaga ett beslut enligt TCO-förordningen och TCO-lagen.....	42
10	Behovet av ändringar i annan lagstiftning.....	42
10.1	Lagen om ansvar för elektroniska anslagstavlor.....	43
10.2	Lagen om elektronisk handel och andra informationssamhällets tjänster	44
10.3	Radio- och tv-lagen	45
11	Ikraftträdande- och övergångsbestämmelser.....	47
12	Konsekvenser.....	48
13	Författningskommentar.....	50
13.1	Förslaget till lag med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online.....	50
13.2	Förslaget till lag om ändring i lagen (1998:112) om ansvar för elektroniska anslagstavlor	56
13.3	Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400).....	57
13.4	Förslaget till lag om ändring i radio- och tv-lagen (2010:696).....	57
Bilaga 1	Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.....	59
Bilaga 2	Sammanfattning av betänkandet EU:s förordning om terrorisminnehåll på internet – kompletteringar och ändringar i svensk rätt (SOU 2022:18).....	90
Bilaga 3	Betänkandets lagförslag.....	93
Bilaga 4	Förteckning över remissinstanserna	100

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online,
2. lag om ändring i lagen (1998:112) om ansvar för elektroniska anslags-
tavlor,
3. lag om ändring i offentlighets- och sekretesslagen (2009:400),
4. lag om ändring i radio- och tv-lagen (2010:696).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online

Härigenom föreskrivs följande.

Lagens innehåll

1 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen).

Termer och uttryck i lagen

2 § Termer och uttryck i denna lag har samma betydelse som i TCO-förordningen.

Behörig myndighet

3 § Den myndighet som regeringen bestämmer är behörig myndighet enligt TCO-förordningen.

Förelägganden

4 § Den behöriga myndigheten får förelägga en värdtjänstleverantör som åsidosätter sina skyldigheter enligt någon av artiklarna 5.1–5.3, 5.5, 7, 10, 15.1 och 17 i TCO-förordningen, i den ursprungliga lydelsen, att vidta sådana åtgärder som krävs för att värdtjänstleverantören ska uppfylla sina skyldigheter.

Ett sådant föreläggande får förenas med vite.

5 § När vite föreläggs ska beloppet bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen, i den ursprungliga lydelsen.

Sanktionsavgifter

6 § Den behöriga myndigheten får besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som åsidosätter sina skyldigheter enligt någon av artiklarna 3.3, 3.6, 4.2, 4.7, 6, 11 och 14.5 i TCO-förordningen, i den ursprungliga lydelsen.

7 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 5 000 000 kronor eller, vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3 i TCO-förordningen, i den

ursprungliga lydelsen, till ett sådant högre belopp som följer av artikel 18.3 i TCO-förordningen, i den ursprungliga lydelsen.

8 § Sanktionsavgiftens storlek ska bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen, i den ursprungliga lydelsen.

9 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Betalning av sanktionsavgifter

10 § En sanktionsavgift ska betalas till den behöriga myndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning enligt lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

11 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Uppgiftsskyldighet

12 § Säkerhetspolisen ska lämna den behöriga myndigheten de uppgifter som den behöriga myndigheten behöver för att fullgöra sitt uppdrag enligt TCO-förordningen.

Säkerhetspolisen har rätt att på begäran ta del av de uppgifter hos den behöriga myndigheten som behövs för att bistå den behöriga myndigheten på det sätt som avses i första stycket.

En uppgift ska inte lämnas om det finns en sekretessbestämmelse som är tillämplig på uppgiften och övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Överklagande

13 § Den behöriga myndighetens beslut enligt TCO-förordningen och denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

1. Denna lag träder i kraft den 1 juli 2023.

2. En sanktionsavgift enligt 6 § får beslutas endast för sådana åsidosättanden av skyldigheter som har skett efter ikraftträdandet.

2.2 Förslag till lag om ändring i lagen (1998:112) om ansvar för elektroniska anslagstavlor

Härigenom föreskrivs att 2 § lagen (1998:112) om ansvar för elektroniska anslagstavlor ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 §

Lagen gäller dock inte

1. tillhandahållande endast av nät eller andra förbindelser för överföring av meddelanden eller av andra anordningar som krävs för att kunna ta i anspråk ett nät eller annan förbindelse,

2. förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern,

3. tjänster som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, *eller*

4. meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare (elektronisk post).

3. tjänster som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen,

4. meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare (elektronisk post), *eller*

5. meddelanden som omfattas av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.

Denna lag träder i kraft den 1 juli 2023.

2.3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att det i offentlighets- och sekretesslagen (2009:400) ska införas en ny paragraf, 35 kap. 23 c §, och närmast före 35 kap. 23 c § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

35 kap.

TCO-förordningen

23 c §

Sekretess gäller hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärende enligt Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och lagen (2023:000) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 juli 2023.

2.4 Förslag till lag om ändring i radio- och tv-lagen (2010:696)

Härigenom föreskrivs att det i radio- och tv-lagen (2010:696) ska införas en ny paragraf, 9 a kap. 14 §, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

9 a kap.

14 §

För leverantörer av videodelningsplattformar gäller även Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och lagen (2023:000) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online.

Denna lag träder i kraft den 1 juli 2023.

3 Ärendet och dess beredning

Den 29 april 2021 antogs Europaparlamentets och rådets förordning (EU) 2021/784 om åtgärder mot spridning av terrorisminnehåll online, nedan kallad TCO-förordningen eller förordningen. Förordningen, som ska tillämpas från och med den 7 juni 2022, finns i *bilaga 1*.

Regeringen beslutade den 15 april 2021 att ge en särskild utredare i uppdrag att föreslå vilken myndighet som bör pekas ut som behörig myndighet enligt TCO-förordningen och vilka sanktioner som ska aktualiseras vid överträdelse av förordningen, samt att analysera i vilken utsträckning förordningen i övrigt medför behov av ändringar eller kompletteringar av svensk rätt.

Utredningen överlämnade den 1 oktober 2021 delbetänkandet EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet (SOU 2021:76). Utredningen föreslog i betänkandet att Polismyndigheten ska utses till behörig myndighet enligt TCO-förordningen. Regeringen beslutade den 28 april 2022 att utse Polismyndigheten till behörig myndighet genom ett tillägg i bilagan till förordningen (2014:1102) med instruktion för Polismyndigheten.

Utredningen överlämnade den 13 april 2022 slutbetänkandet EU:s förordning om terrorisminnehåll på internet – kompletteringar och ändringar i svensk rätt (SOU 2022:18). I betänkandet föreslås bland annat en ny lag med kompletterande bestämmelser till TCO-förordningen. En sammanfattning av betänkandet finns i *bilaga 2*. Betänkandets lagförslag finns i *bilaga 3*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2022/01400).

I denna lagrådsremiss behandlas förslagen i slutbetänkandet.

4 TCO-förordningens syfte och huvudsakliga innehåll

Förordningens bakgrund och syfte

Flera av de senaste årens terrorattentat i Europa har haft digitala inslag. I vissa fall har gärningspersonen eller en annan person direktsänt terrorattentatet på internet eller förhålligt gärningen i efterhand på internet. Det har även förekommit att gärningspersoner före ett attentat radikaliserats med hjälp av innehåll på internet och fått tillgång till instruktioner för genomförande av attentat eller tillverkning av hjälpmedel. Som ett led i arbetet mot terrorism har EU vidtagit olika åtgärder för att motverka spridningen av terrorisminnehåll på internet. TCO-förordningen är ett resultat av det arbetet.

Förordningen innehåller regler för att åtgärda missbruk av värdtjänster för spridning av terrorisminnehåll online till allmänheten (artikel 1.1). Förordningens övergripande syfte så som det kommer till uttryck i skälen till förordningen 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 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 (skäl 1).

Förordningens tillämpningsområde och vissa definitioner

TCO-förordningen är tillämplig på värdtjänstleverantörer som erbjuder tjänster i EU, oberoende av deras huvudsakliga verksamhetsställe, i den mån de sprider information till allmänheten (artikel 1.2).

Begreppet värdtjänstleverantör är alltså centralt. Det definieras, delvis genom en hänvisning, som en leverantör av någon av alla informations-samhällets tjänster som består i att information som tillhandahållits av en innehållsleverantör lagras på dennes begäran (artikel 2.1). Med informationssamhällets tjänster avses tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I skälen till förordningen utvecklas begreppet något: Förordningen bör tillämpas på sådana leverantörer av informations-samhällets 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 är av rent teknisk, automatisk och passiv karaktär. Begreppet lagring bör förstås som förvaring av data i minnet hos en fysisk eller virtuell server (skäl 13). Det innebär att förordningen exempelvis bör omfatta leverantörer av sociala medietjänster, video-, bild- och ljudspelningstjänster, samt fildelningstjänster och andra molntjänster, i den mån dessa tjänster används för att göra den lagrade informationen tillgänglig för allmänheten på direkt begäran av innehållsleverantören (skäl 14).

En värdtjänstleverantör behöver inte ha sitt huvudsakliga verksamhetsställe i unionen för att förordningen ska vara tillämplig, utan det är tillräckligt att leverantören erbjuder tjänster i unionen. Med detta avses att 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 (artikel 2.4). Betydande anknytning innebär i sin tur att en värdtjänstleverantör har en anknytning till en eller flera medlemsstater som följer antingen av dennes verksamhetsställe i unionen eller av särskilda faktiska kriterier. Dessa kriterier kan vara att värdtjänstleverantören har ett betydande antal användare av dess tjänster i en eller flera medlemsstater eller att verksamheten är riktad mot en eller flera medlemsstater (artikel 2.5). En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen ska skriftligen utse en fysisk eller juridisk person till sin rättsliga företrädare i unionen (artikel 17.1).

För att förordningen ska vara tillämplig krävs också att det är fråga om spridning till allmänheten. Detta definieras i förordningen som tillgängliggörande av information på begäran av en innehållsleverantör – dvs. en användare (av en värdtjänst) som har tillhandahållit information som

lagras eller sprids – för ett potentiellt obegränsat antal personer (artikel 2.2 och 2.3). Av skälen till förordningen framgår att detta innebär att information görs lätt tillgänglig för användare i allmänhet utan att det krävs någon ytterligare åtgärd från innehållsleverantörens sida, oberoende av om dessa personer verkligen tar del av informationen i fråga. Om tillgång till informationen 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 (skäl 14).

Ett ytterligare begrepp som är av stor relevans vid tillämpningen av förordningen är terrorisminnehåll, som i förordningen knyts till den straffrättsliga definitionen av terroristbrott i Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism (terrorismdiriktivet). Terrorisminnehåll definieras således som material som a) anstiftar till begåendet av ett av de brott som avses i artikel 3.1 a–i i terrorismdiriktivet, om sådant material, direkt eller indirekt, såsom genom förhållande 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 terrorismdiriktivet 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 terrorismdiriktivet, 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 terrorismdiriktivet eller e) utgör ett hot om begående av ett av de brott som avses i artikel 3.1 a–i i terrorismdiriktivet (artikel 2.7). Material som sprids till allmänheten i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forsknings-syfte 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 emellertid inte anses vara terrorisminnehåll (artikel 1.3).

En ytterligare begränsning av tillämpningsområdet anger att förordningen inte ska 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 (artikel 1.4).

Förordningens huvudsakliga innehåll

Varje medlemsstat ska utse en eller flera s.k. behöriga myndigheter som förses med ett antal befogenheter enligt förordningen – den behöriga myndigheten kan bl.a. utfärda och granska avlägsnandeordrar, övervaka genomförandet av specifika åtgärder och påföra sanktioner (artikel 12.1). I enlighet med detta har regeringen, genom ett tillägg i bilagan till förordningen (2014:1102) med instruktion för Polismyndigheten, utsett

Polismyndigheten till svensk behörig myndighet med verkan från det att TCO-förordningen började tillämpas den 7 juni 2022.

En avlägsnandeorder innebär en skyldighet för en värdtjänstleverantör att avlägsna terrorisminnehåll eller göra det oåtkomligt i samtliga medlemsstater. Detta ska ske så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern (artikel 3). En avlägsnandeorder kan enligt förordningen riktas även till en värdtjänstleverantör som varken har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i den medlemsstat där den utfärdande behöriga myndigheten är belägen. I sådana fall ska den utfärdande myndigheten samtidigt översända en kopia av avlägsnandeordern till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare, och den mottagande behöriga myndigheten har då möjlighet att granska ordern och under vissa förhållanden fastställa att den är oförenlig med TCO-förordningen eller de grundläggande rättigheter och friheter som garanteras i EU:s stadga om de grundläggande rättigheterna (artikel 4).

En värdtjänstleverantör som är exponerad för terrorisminnehåll ska vidta specifika åtgärder för att motverka spridning av sådant innehåll (artikel 5). Det är den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad som prövar om en leverantör ska anses exponerad för terrorisminnehåll. Ett beslut om exponering ska grundas på objektiva faktorer, till exempel att värdtjänstleverantören under de föregående tolv månaderna har mottagit två eller fler avlägsnandeorder (artikel 5.4). En värdtjänstleverantör som anses exponerad för terrorisminnehåll ska, i tillämpliga fall, i sina användarvillkor inkludera och tillämpa bestämmelser om åtgärder mot missbruk av dess tjänster för spridning av terrorisminnehåll (artikel 5.1). I övrigt beslutar värdtjänstleverantören själv vilka specifika åtgärder som ska vidtas – i förordningen ges enbart exempel på vad dessa kan innebära – men de måste på ett effektivt sätt minska graden av exponering och dessutom bl.a. vara riktade och proportionella (artikel 5.2 och 5.3). De specifika åtgärderna ska rapporteras till den behöriga myndigheten och om denna inte anser att åtgärderna uppfyller förordningens krav kan den behöriga myndigheten besluta att värdtjänstleverantören ska vidta nödvändiga åtgärder (artikel 5.5 och 5.6).

Förordningen innehåller även vissa ytterligare krav på värdtjänstleverantörerna, bl.a. när det gäller transparens (artikel 7) och information till innehållsleverantörer (artikel 11), samt krav på de behöriga myndigheterna, bl.a. när det gäller transparens (artikel 8) och samarbete med andra behöriga myndigheter och Europol (artikel 14). Dessutom kräver förordningen att medlemsstaterna ska säkerställa att en värdtjänstleverantör eller en innehållsleverantör som tar emot vissa beslut har rätt till effektiva rättsmedel (artikel 9) samt att det ska finnas ett nationellt sanktionssystem vid vissa överträdelser av förordningen (artikel 18).

Möjligheten att använda frivilliga åtgärder

Som utredningen redogjort för har myndigheter i andra medlemsstater redan före TCO-förordningens ikraftträdande arbetat mot spridning av

terrorisminnehåll på internet genom olika former av frivilliga åtgärder, exempelvis genom att värdtjänstleverantörer uppmärksammas på specifikt innehåll som kan strida mot deras användarvillkor (kapitel 6 i SOU 2022:18). Det kan därför finnas anledning att notera att det av skälen i ingressen till TCO-förordningen framgår att denna inte är avsedd att hindra medlemsstaterna från att även fortsättningsvis vidta den typen av åtgärder (skäl 40). Det bör alltså vara möjligt för en behörig myndighet att, innan åtgärder enligt förordningen vidtas, via en mer informell kontakt med en värdtjänstleverantör uppmärksamma denne på visst innehåll. Som utredningen framhåller är det grundläggande att sådana eventuella kontakter endast sker inom de ramar som tryck- och yttrandefriheten tillåter och på ett sådant sätt att åtgärden inte uppfattas som tvingande av värdtjänstleverantören.

5 En ny lag som kompletterar TCO-förordningen

5.1 En ny lag med bestämmelser som kompletterar TCO-förordningen ska införas

Regeringens förslag: En ny lag med bestämmelser som kompletterar TCO-förordningen ska införas. Den ska benämnas lagen med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online.

Termer och uttryck i den nya lagen ska ha samma betydelse som i TCO-förordningen.

De hänvisningar till TCO-förordningen som ger bestämmelserna i den nya lagen materiellt innehåll ska vara statiska.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Myndigheten för press, radio och tv, Sveriges advokatsamfund och TechSverige* uppmärksammar att det finns oklarheter i TCO-förordningens definitioner, särskilt av begreppet värdtjänstleverantör. Det kan därför vara svårt att bedöma om en enskild aktör omfattas av förordningen eller inte. *Förvaltningsrätten i Jönköping* anser att det finns frågor om domsrätt som bl.a. relaterar till oklarheten när det gäller begreppet värdtjänstleverantör och som bör belysas ytterligare.

Skälen för regeringens förslag: En EU-förordning är direkt tillämplig i medlemsstaterna och ska därför inte genomföras i den nationella rätten. I regel behöver medlemsstaterna inte heller införa kompletterande nationella bestämmelser till en EU-förordning. Detta kan dock bli aktuellt om en förordning överlämnar vissa frågor åt medlemsstaterna. Dessutom har medlemsstaterna en skyldighet att se till att en EU-förordning kan tillämpas i praktiken och få ett effektivt genomslag i medlemsstaten. I vissa fall förutsätter en EU-förordning därför att medlemsstaterna inför nationella regler.

TCO-förordningen överlämnar vissa frågor till medlemsstaterna att reglera. Det handlar främst om vilken myndighet som ska vara behörig myndighet, vilka sanktioner som ska kunna tillämpas vid överträdelse av förordningen och om att säkerställa rätten till effektiva rättsmedel. Dessutom kräver en effektiv tillämpning av förordningen att den behöriga myndigheten har tillgång till nödvändig information – något som kan innebära ett behov av bestämmelser som möjliggör uppgiftsutbytet.

Det står därmed klart att det kommer att behövas vissa nationella bestämmelser som kompletterar TCO-förordningen. Dessa bör enligt regeringen samlas i en ny lag. För att göra det tydligt att den nya lagen inte är heltäckande, utan endast ett komplement till TCO-förordningen, bör den benämnas lagen med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online (fortsättningsvis benämnd TCO-lagen).

Som flera remissinstanser, bl.a. *Sveriges advokatsamfund* och *Förvaltningsrätten i Jönköping*, har påtalat är förordningens definitioner, även när de läses med de förtydliganden som görs i skälen, inte helt tydliga. Detta gäller även definitionen av begreppet värdtjänstleverantör och det är därmed inte alla gånger givet om en viss aktör omfattas av förordningen eller inte. Med hänsyn till att TCO-förordningen är direkt tillämplig EU-rätt saknas emellertid utrymme för regeringen att föreslå förtydliganden av begreppen i svensk rätt. Som utredningen föreslår bör TCO-lagen i stället innehålla en upplysning om att termer och uttryck i lagen har samma betydelse som i TCO-förordningen. Hur förordningen, inklusive dess bestämmelser om jurisdiktion, ska tolkas är en fråga för de nationella myndigheter och domstolar som ska tillämpa förordningen, och ytterst för EU-domstolen. Som vägledning kan det noteras att utredningen för ett resonemang om hur begreppet värdtjänstleverantör ska förstås och ger exempel på vilka tjänster som kan omfattas av förordningen (avsnitt 4.3 i SOU 2022:18, se särskilt avsnitt 4.3.4).

För att undvika dubbelreglering kommer TCO-lagen att behöva innehålla hänvisningar till bestämmelser i TCO-förordningen. Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En följd av denna hänvisningsteknik är därmed att den nationella författningen normalt behöver ändras varje gång EU-bestämmelsen ändras. En dynamisk hänvisning innebär i stället att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. TCO-lagen kommer att innehålla bestämmelser om sanktioner vid vissa överträdelse av förordningen. Dessa bestämmelser bör innehålla statiska hänvisningar till TCO-förordningen.

5.2 En bestämmelse om behörig myndighet

<p>Regeringens förslag: Det ska framgå av TCO-lagen att den myndighet som regeringen bestämmer är behörig myndighet enligt TCO-förordningen.</p>

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna har inte lämnat några synpunkter på förslaget.

Skälen för regeringens förslag: Som framgår av kapitel 4 ska varje medlemsstat utse en eller flera s.k. behöriga myndigheter enligt TCO-förordningen. I enlighet med detta har regeringen, med stöd av dess s.k. restkompetens enligt 8 kap. 7 § första stycket 2 regeringsformen, genom ett tillägg i bilagan till förordningen med instruktion för Polismyndigheten utsett Polismyndigheten till svensk behörig myndighet. Även om det alltså inte krävts lagstöd för att peka ut den behöriga myndigheten anser regeringen att TCO-lagen bör innehålla en upplysning om att den myndighet som regeringen bestämmer är behörig myndighet enligt TCO-förordningen. Den samlade regleringen blir på så vis tydligare, inte minst eftersom TCO-lagen kommer att innehålla ett antal bestämmelser som direkt hänför sig till den behöriga myndigheten.

6 Förhållandet till yttrande- och informationsfrihet

6.1 Skyddet för yttrande- och informationsfrihet

Ett syfte med TCO-förordningen är att motverka spridning av terrorism-innehåll, dvs. spridning av vissa yttranden och annan information. När regler med sådant syfte föreslås uppkommer frågan hur dessa förhåller sig till bestämmelserna om rätt till yttrande- och informationsfrihet. I svensk rätt regleras dessa rättigheter främst i regeringsformen, tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Därutöver regleras rättigheterna i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga).

Europakonventionen och EU:s rättighetsstadga

Enligt artikel 10.1 i Europakonventionen har var och en rätt till yttrandefrihet. Denna rätt innefattar åsiktsfrihet samt frihet att ta emot och sprida uppgifter och tankar utan offentlig myndighets inblandning och oberoende av territoriella gränser. Under vissa förutsättningar kan rätten till yttrandefrihet begränsas enligt artikel 10.2. En begränsning måste göras i lag och vara nödvändig i ett demokratiskt samhälle, med hänsyn till exempelvis statens säkerhet eller den allmänna säkerheten eller till förebyggande av oordning eller brott. Rätten till yttrandefrihet i artikel 11 i EU:s rättighetsstadga är snarlikt formulerad. Även denna rätt kan, enligt artikel 52.1, begränsas genom lag, om begränsningen är nödvändig och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter. För åtgärder som begränsar rätten till yttrandefrihet gäller enligt både Europakonventionen och EU:s rättighetsstadga ett krav på proportionalitet. Det innebär att en avvägning ska göras mellan å ena sidan den enskildes

intresse av yttrandefrihet och å andra sidan det allmänna eller enskilda intresse som motiverar begränsningen.

Regeringsformen

I regeringsformen tillförsäkras var och en, gentemot det allmänna, bl.a. yttrande- och informationsfrihet. Av den allmänna regleringen av rätten till yttrandefrihet följer att den svenska folkstyrelsen bygger på en fri åsiktsbildning och att var och en gentemot det allmänna är tillförsäkrad frihet att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor (1 kap. 1 § andra stycket och 2 kap. 1 § första stycket 1). Av den senare bestämmelsens andra punkt framgår även rätten till informationsfrihet, dvs. friheten att inhämta och ta emot upplysningar samt att i övrigt ta del av andras yttranden.

Yttrandefriheten i regeringsformen är generellt utformad och innehåller en hänvisning till tryckfrihetsförordningen och yttrandefrihetsgrundlagen rörande tryckfrihet och motsvarande frihet att yttra sig i radio, tv och i vissa liknande överföringar, offentliga uppspelningar ur en databas samt filmer, videogram, ljudupptagningar och andra tekniska upptagningar (2 kap. 1 § andra stycket). Hänvisningen innebär att tryckfriheten enligt tryckfrihetsförordningen och motsvarade yttrandefrihet enligt yttrandefrihetsgrundlagen undantas från regeringsformens tillämpningsområde. Bestämmelserna om yttrande- och informationsfrihet i regeringsformen är alltså tillämpliga när det inte är fråga om friheten att yttra sig i de medier som faller inom tryckfrihetsförordningens eller yttrandefrihetsgrundlagens tillämpningsområde.

Yttrande- och informationsfriheten enligt regeringsformen är inte absolut utan kan begränsas genom lag under vissa förutsättningar (2 kap. 20 § första stycket 1). Till att börja med får en begränsning endast ske för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 21 §). Liksom enligt Europakonventionen och EU:s rättighetsstadga gäller alltså även enligt regeringsformen ett krav på proportionalitet vid inskränkningar av yttrande- och informationsfriheten. Utöver dessa grundläggande krav gäller att yttrande- och informationsfriheten enbart får begränsas med hänsyn till rikets säkerhet, folkförsörjningen, allmän ordning och säkerhet, enskildas anseende, privatlivets helgd eller förebyggandet och beivrandet av brott, eller i övrigt om särskilt viktiga skäl föranleder det (2 kap. 23 § första stycket). När lagstiftaren överväger en begränsning ska vikten av vidaste möjliga yttrande- och informationsfrihet i politiska, religiösa, fackliga, vetenskapliga och kulturella angelägenheter särskilt beaktas (2 kap. 23 § andra stycket).

Tryckfrihetsförordningen

Den särskilda grundlagsregleringen i tryckfrihetsförordningen omfattar skrifter som framställs i tryckpress och, om vissa förutsättningar är uppfyllda, skrifter som har mångfaldigats genom fotokopiering eller liknande teknik (1 kap. 2 §). Inom lagens tillämpningsområde gäller både

ett censurförbud och den s.k. exklusivetsprincipen, som innebär att ingripanden på grund av missbruk av tryckfriheten endast får göras i de fall som anges i tryckfrihetsförordningen (1 kap. 8 och 9 §§).

Tryckfrihetsförordningen kan i vissa fall bli tillämplig även på publiceringar på internet om det är fråga om innehåll i en tryckt periodisk skrift som är skyddad enligt tryckfrihetsförordningen och som i oförändrat skick publiceras på internet. En sådan publicering kan under vissa förutsättningar omfattas av grundlagsskyddet i tryckfrihetsförordningen enligt de s.k. bilagereglerna (1 kap. 5–6 §§). Sådana program som tillhandahålls ur en databas och därmed publiceras på internet faller dock som huvudregel inom tillämpningsområdet för yttrandefrihetsgrundlagen.

Yttrandefrihetsgrundlagen

Den särskilda grundlagsregleringen i yttrandefrihetsgrundlagen är i huvudsak tillämplig på två olika kommunikationstekniker. Den första kategorin avser ”ljudradio, tv och vissa liknande överföringar”, eller annorlunda uttryckt traditionella radio- och tv-sändningar, webbsändningar samt viss annan publicering på internet. Den andra kategorin omfattar fysiska informationsbärare, till exempel filmer och upptagningar på band (1 kap. 1 § första stycket). All kommunikation som sker med dessa tekniker omfattas emellertid inte av grundlagen, utan frågan om huruvida den är tillämplig eller inte bestäms av ett tämligen detaljerat regelverk i 1 kap.

Yttrandefrihetsgrundlagen har utformats med tryckfrihetsförordningen som förebild och innehåller flera principer som även kommer till uttryck i den, till exempel förbudet mot censur och exklusivetsprincipen. Censurförbudet innebär bl.a. att det inte är tillåtet för en myndighet eller ett annat allmänt organ att på grund av innehållet förbjuda eller hindra framställning, offentliggörande eller spridning bland allmänheten av ett program eller en teknisk upptagning, om åtgärden inte har stöd i yttrandefrihetsgrundlagen (1 kap. 11 §). Exklusivetsprincipen innebär att en myndighet eller ett annat allmänt organ inte utan stöd i yttrandefrihetsgrundlagen får ingripa mot någon för att han eller hon i ett program eller en teknisk upptagning har missbrukat yttrandefriheten eller medverkat till ett sådant missbruk, eller av sådan anledning ingripa mot programmet eller upptagningen (1 kap. 14 §).

Publiceringar på internet faller som utgångspunkt utanför yttrandefrihetsgrundlagens tillämpningsområde. Det innebär att grundlagsskyddet i stället finns i regeringsformen. Från denna huvudregel görs dock undantag genom webbsändningsregeln (1 kap. 3 § andra stycket) och databasregeln (1 kap. 4 §). Databasregeln ger under vissa förutsättningar grundlagsskydd för yttranden som sker genom tillhandahållanden till allmänheten ur databaser. För vissa aktörer gäller grundlagsskyddet automatiskt. Så är fallet för bl.a. redaktioner för periodiska skrifter, t.ex. en tidningsredaktion, och för massmedieföretag, t.ex. en nyhetsbyrå. Andra aktörer har möjlighet att ansöka om utgivningsbevis för verksamheten och på så sätt få ett s.k. frivilligt grundlagsskydd (1 kap. 5 §).

6.2 TCO-förordningens förhållande till skyddet för yttrande- och informationsfrihet

Regeringens bedömning: TCO-förordningen är inte tillämplig i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Detsamma gäller därmed för TCO-lagen.

Bestämmelserna i TCO-förordningen och TCO-lagen är förenliga med regeringsformens bestämmelser om yttrande- och informationsfrihet.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Justitiekanslern* anser att slutsatsen att TCO-förordningen enligt unionsrätten inte behöver tillämpas i den utsträckning det skulle strida mot de nationella mediegrundlagarna inte framstår som självklar. Det är enligt Justitiekanslern därmed oklart bl.a. om den svenska behöriga myndigheten, i en situation där ett visst publicerat innehåll bedöms vara skyddat av de svenska grundlagarna, kan underlåta att utfärda en avlägsnandeorder på det sätt som förordningen kräver utan att överträda unionsrätten. *Myndigheten för press, radio och tv* delar bedömningen att bestämmelserna i TCO-förordningen utgör en godtagbar begränsning av yttrande- och informationsfriheten i regeringsformen. Myndigheten pekar vidare på att de svenska mediegrundlagarna skulle kunna komma att skydda innehåll som sprids på internet med andra syften än de godtagbara syften som medför att material undantas från förordningens tillämpningsområde och ser en risk att förordningen skulle kunna kringgås genom att någon som vill sprida terrorisminnehåll på sin webbplats söker utgivningsbevis för den. *Sveriges advokatsamfund* delar uppfattningen att innehåll som skyddas av mediegrundlagarna ska vara undantaget från TCO-förordningens tillämpningsområde, men konstaterar samtidigt att skäl 12 i förordningen anger bl.a. att syftet med publiceringen ”bör” beaktas. Enligt samfundet är detta inte godtagbart, och samfundet anser därför att kompletteringslagen ska kompletteras med ett avsnitt som dels klargör att TCO-förordningen inte är tillämplig på värdtjänstleverantörer som omfattas av tryckfrihetsförordningen och yttrandefrihetsgrundlagen, dels kodifierar skäl 12 som en ”ska-regel”. *Tidningsutgivarna* tillstyrker bedömningen att TCO-förordningen och kompletteringslagen i förhållande till yttrande- och informationsfriheten i svensk rätt – dvs. tryckfrihetsförordningen och yttrandefrihetsgrundlagen – inte är tillämpliga och därför inte påverkar det grundlagsskyddade området i svensk rätt. *Tidningsutgivarna* understryker vidare att även sådant journalistiskt innehåll som formellt inte omfattas av skyddet i mediegrundlagarna, utan av det allmänna skyddet för yttrande- och informationsfriheten i regeringsformen, kan omfattas av undantaget i förordningen för innehåll som sprids i visst syfte.

Skälen för regeringens bedömning

Material som sprids i visst syfte är undantaget från TCO-förordningen

Artikel 1.3 i TCO-förordningen innehåller ett för yttrande- och informationsfriheten grundläggande undantag. Enligt bestämmelsen ska 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, inte anses vara terrorisminnehåll. Det innebär att sådant material inte kan bli föremål för någon åtgärd enligt TCO-förordningen även om det uppfyller kraven på terrorisminnehåll i artikel 2.7. Undantaget träffar både material som omfattas av skyddet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen (mer om dessa grundlagar nedan) och sådant annat material, som *Tidningsutgivarna* pekar på, som omfattas av det allmänna skyddet för yttrande- och informationsfrihet i regeringsformen. Det kan noteras att bestämmelsen i artikel 1.3 innehåller en sådan ”ska-regel” som *Sveriges advokatsamfund* efterfrågat – det finns därför inget behov av att överväga införandet av en sådan i TCO-lagen.

Förhållandet mellan TCO-förordningen och mediegrundlagarna

Bestämmelserna i TCO-förordningen gäller som framgått terrorisminnehåll, dvs. en viss typ av material på internet som lagras av en värdtjänstleverantör på begäran av en innehållsleverantör och som är tillgängligt för allmänheten. Som redogjorts för i avsnitt 6.1 kan samtidigt material som publiceras på internet i vissa fall omfattas av tryckfrihetsförordningen eller, framför allt, yttrandefrihetsgrundlagen (nedan benämnda mediegrundlagarna). Regeringen delar utredningens bedömning att material som kan bli föremål för prövning enligt TCO-förordningen – material som alltså inte omfattas av det ovan nämnda undantaget i artikel 1.3 – i vissa fall kan vara tillhandahållna på medier som omfattas av mediegrundlagarna.

TCO-förordningens tillämpningsområde begränsas emellertid även av bestämmelsen i artikel 1.4. Av den följer att förordningen inte ska medföra någon ändring av skyldigheten att respektera de rättigheter, friheter och principer som avses i artikel 6 i EU-fördraget (som hänvisar till EU:s rättighetsstadga) och ska tillämpas utan att det påverkar tillämpningen av grundläggande principer som rör yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald. Som *Justitiekanslern* påpekat är det inte självklart att skyddet för yttrande- och informationsfriheten enligt unionsrätten motsvarar skyddet i de svenska mediegrundlagarna. Såsom artikel 1.4 är uppbyggd är hänvisningen till grundläggande principer som rör yttrande- och informationsfrihet i bestämmelsens andra led emellertid inte begränsad till att endast avse unionsrättsliga principer. Regeringen delar därför utredningens bedömning att rätten till yttrande- och informationsfrihet såsom den kommer till uttryck i de svenska mediegrundlagarna utgör ett uttryck för sådana principer som omfattas av artikel 1.4.

Tillämpningen av mediegrundlagarna ska alltså inte påverkas av TCO-förordningen. Det innebär att TCO-förordningen och TCO-lagen inte ska tillämpas i den utsträckning detta skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Innehåll som skyddas av någon av mediegrundlagarna kan därför inte bli föremål för någon åtgärd med stöd av TCO-förordningen eller TCO-lagen, exempelvis kan en avlägsnandebefallning inte utfärdas avseende sådant material. Något skäl för att, såsom

Sveriges advokatsamfund föreslagit, föra in en särskild bestämmelse om detta i TCO-lagen finns enligt regeringen inte.

Myndigheten för press, radio och tv har i sammanhanget pekat på att de svenska mediegrundlagarna – främst möjligheterna till s.k. frivilligt grundlagsskydd genom utgivningsbevis – skulle kunna komma att skydda innehåll som sprids på internet med andra syften än de som enligt artikel 1.3 medför att material undantas från förordningens tillämpningsområde. Regeringen behandlar dock inte utformningen av de svenska mediegrundlagarna i detta lagstiftningsärende.

TCO-förordningen och TCO-lagen är förenliga med regeringsformens bestämmelser om yttrande- och informationsfrihet

Material som är föremål för prövning enligt TCO-förordningen och som inte omfattas av skyddet i någon av mediegrundlagarna, omfattas i stället av det allmänna skyddet för yttrande- och informationsfrihet i regeringsformen. De åtgärder som kan vidtas med stöd av förordningen och TCO-lagen innebär inskränkningar i innehållsleverantörens yttrandefrihet och mottagarnas informationsfrihet. Som framgått är yttrande- och informationsfriheten enligt regeringsformen emellertid inte absolut utan kan begränsas genom lag (ett begrepp som också omfattar EU-förordningar), under förutsättning att det rör sig om en proportionerlig inskränkning som sker i ett godtagbart syfte.

Som utredningen konstaterat är den begränsning av yttrande- och informationsfriheten som TCO-förordningen innebär motiverad av flera angelägna syften, såsom att skydda Sveriges säkerhet, att upprätthålla allmän ordning och säkerhet samt att förebygga brott. Dessutom innehåller förordningen, som framgått, undantag för material som sprids i vissa syften samt det särskilda skydd som uttrycks i artikel 1.4. Sammantaget innebär detta enligt regeringen att bestämmelserna i TCO-förordningen och den kompletterande TCO-lagen utgör en godtagbar begränsning av yttrande- och informationsfriheten enligt regeringsformen. Detsamma gäller motsvarande skydd enligt Europakonventionen och EU:s rättighetsstadga.

Något om den behöriga myndighetens prövning

Det är den behöriga myndigheten som ska avgöra om TCO-förordningen kan tillämpas på visst material eller inte. För att kunna bedöma detta kan den behöriga myndigheten, i enlighet med vad som angetts ovan, bl.a. behöva utreda syftet med publiceringen samt kontrollera om innehållet omfattas av någon av mediegrundlagarna. I utredningen ges viss vägledning för genomförandet av en sådan bedömning (SOU 2022:18 s. 77 f.).

Som utredningen anger kan skyddet för yttrande- och informationsfrihet i mediegrundlagarna även få betydelse när en behörig myndighet i en annan medlemsstat handlägger ett ärende eller utfärdar en avlägsnandeorder mot en värdtjänstleverantör som har sitt huvudsakliga verksamhetsställe i Sverige eller sin rättsliga företrädare bosatt eller etablerad här. För att undvika att material som omfattas av skyddet i någon av mediegrundlagarna i sådana fall blir föremål för en avlägsnandeorder bör den svenska behöriga myndigheten ha möjlighet att, i enlighet med

artikel 14 om samarbete mellan behöriga myndigheter, informera sin utländska motsvarighet om innebörden av det svenska grundlagsskyddet. Skulle en avlägsnandeorder ändå utfärdas i en annan medlemsstat har den svenska behöriga myndigheten möjlighet att initiera ett granskningsförfarande enligt artikel 4 och bl.a. pröva om ordern på ett uppenbart sätt är oförenlig med TCO-förordningen.

7 Sanktioner

7.1 TCO-förordningens krav på sanktioner

Enligt artikel 18.1 i TCO-förordningen ska medlemsstaterna fastställa regler om sanktioner för värdtjänstleverantörers överträdelser av vissa utpekade bestämmelser i förordningen och vidta alla åtgärder som krävs för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

I artikel 18.2 finns bestämmelser om att medlemsstaterna ska säkerställa att de behöriga myndigheterna beaktar alla relevanta omständigheter när de beslutar huruvida en sanktion ska påföras och när de fastställer sanktionernas typ och nivå. Artikel 18.3 innehåller också en icke-uttömmande uppräkningslista av ett antal sådana omständigheter. I artikel 18.3 finns vidare en särskild skyldighet för medlemsstaterna att säkerställa att en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3, dvs. att avlägsna terrorisminnehåll eller göra det oåtkomligt efter mottagande av en avlägsnandeorder, blir föremål för böter på upp till fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret.

7.2 TCO-förordningens krav bör uppfyllas genom bestämmelser om administrativa sanktioner

Regeringens bedömning: Överträdelser av TCO-förordningen bör inte kriminaliseras, utan bör leda till administrativa sanktioner i form av antingen vitesföreläggande eller sanktionsavgift.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna har inte lämnat några synpunkter på bedömningen.

Skälen för regeringens bedömning: Av skälen i TCO-förordningen framgår att sanktioner i förordningens mening kan vara av administrativ eller straffrättslig art (skäl 45). Förordningen ställer alltså inte upp något krav på att överträdelser av bestämmelserna i förordningen ska vara straffbelagda. Detta gäller även sådana överträdelser som avses i artikel 18.3, trots att det i den svenska texten där talas om ”böter” (jfr ”financial penalties” i den engelska texten). Vad förordningen däremot kräver är att sanktionerna ska vara effektiva, proportionella och avskräckande.

Kravet på sanktioner avser värdtjänstleverantörers överträdelser av bestämmelser i förordningen. Såväl en fysisk som en juridisk person kan vara

en värdtjänstleverantör i förordningens mening, men som utredningen konstaterat är merparten av de berörda värdtjänstleverantörerna juridiska personer. För att leva upp till förordningens krav är det därför viktigt att de sanktioner som införs är effektiva och avskräckande i förhållande till både fysiska och juridiska personer.

Även om juridiska personer inte kan åläggas straffansvar, så kan de åläggas företagsbot enligt 36 kap. 7 § brottsbalken. Merparten av de överträdelse av TCO-förordningen som måste kunna leda till sanktioner är emellertid av mer administrativ karaktär och redan av det skälet inte aktuella att kriminalisera. För att åstadkomma ett effektivt sanktions-system bör detta dessutom bygga på ett i grunden strikt ansvar (se vidare avsnitt 7.4.1), dvs. en ansvarsform som inte förekommer i straffrätten. Regeringen gör därför, liksom utredningen, bedömningen att kriminalisering av överträdelse av bestämmelser i TCO-förordningen inte är ett lämpligt sätt att genomföra kravet på sanktioner i artikel 18.1.

Vad som då återstår är ett system med sanktioner av administrativ art. Sådana sanktioner kan riktas mot såväl fysiska som juridiska personer och det är i regel möjligt att åstadkomma ett snabbt och effektivt förfarande. Dessutom kan sanktionerna anpassas både efter vilken skyldighet som åsidosatts och vem det är som ska påföras sanktionen. Regeringen gör därför bedömningen att administrativa sanktioner kan utgöra ett effektivt och avskräckande, men samtidigt proportionellt, styrmedel gentemot värdtjänstleverantörer oavsett om dessa är fysiska eller juridiska personer och oberoende av verksamheternas storlek.

Som utredningen konstaterat är det i praktiken två typer av administrativa sanktioner som kan vara aktuella: beslut om förelägganden som förenas med vite (vitesförelägganden) och sanktionsavgifter. Vitesförelägganden är framåtsyftande, dvs. de ska få mottagaren att vidta vissa handlingar, och kan därför sägas vara handlingsdirigerande. Sanktionsavgifter aktualiseras däremot först när en överträdelse har ägt rum och har därför en mer avskräckande och bestraffande funktion.

Flera av de bestämmelser i TCO-förordningen som ska vara förenade med sanktioner innehåller skyldigheter för värdtjänstleverantörer att vidta åtgärder för att utforma sina värdtjänster så att förekomsten av terrorisminnehåll motverkas. Underlåter en värdtjänstleverantör att uppfylla krav av det slaget behövs i första hand ett handlingsdirigerande verktyg. Regeringen delar därför utredningens bedömning att den behöriga myndigheten i de fallen bör ges möjlighet att förelägga värdtjänstleverantören att vidta åtgärder så att denne uppfyller förordningens krav och förena sådana förelägganden med vite.

Vitesförelägganden är emellertid inte lämpliga vid alla överträdelse av TCO-förordningen. Följer en värdtjänstleverantör exempelvis inte en avlägsnandeorder är ett vitesföreläggande mindre verkningsfullt. I stället bör överträdelse av den typen föranleda sanktioner med en bestraffande funktion – i sådana fall framstår alltså sanktionsavgift som ett lämpligare val.

7.3 Vitesförelägganden

7.3.1 Den behöriga myndigheten ska kunna besluta om vitesföreläggande

Regeringens förslag: Den behöriga myndigheten ska få förelägga en värdtjänstleverantör som åsidosätter sina skyldigheter enligt någon av artiklarna 5.1–5.3, 5.5, 7, 10, 15.1 och 17 i TCO-förordningen att vidta sådana åtgärder som krävs för att värdtjänstleverantören ska uppfylla sina skyldigheter.

Ett sådant föreläggande får förenas med vite.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår att det i lagtexten ska anges vilka åtgärder som förelägganden kopplade till respektive artikel kan avse.

Remissinstanserna: *Myndigheten för press, radio och tv (MPRT)* påpekar att det finns en viss potentiell överlappning mellan den behöriga myndighetens möjligheter att besluta om vitesföreläggande och den egna myndighetens tillsyn och föreläggandemöjligheter när det gäller videodelningsplattformar och lämpliga åtgärder enligt radio- och tv-lagen (2010:696). Myndigheten ser därför fördelar med att den och den behöriga myndigheten samverkar i frågor som rör leverantörer av videodelningsplattformar. Övriga remissinstanser har inga synpunkter på förslaget.

Skälen för regeringens förslag: Som framgår av föregående avsnitt innehåller flera av de bestämmelser i TCO-förordningen som enligt artikel 18 ska vara förenade med sanktioner skyldigheter av sådant slag att den behöriga myndigheten i första hand behöver ett handlingsdirigerande verktyg när en värdtjänstleverantör inte uppfyller kraven.

Regeringen, liksom utredningen, gör till att börja med bedömningen att bestämmelserna i artikel 5.1–5.3 och 5.5 är av detta slag. Bestämmelserna gäller värdtjänstleverantörer som enligt artikel 5.4 är exponerade för terrorisminnehåll. En sådan värdtjänstleverantör ska i sina användarvillkor inkludera bestämmelser om åtgärder mot missbruk av dess tjänster för spridning till allmänheten av terrorisminnehåll och tillämpa dessa bestämmelser (artikel 5.1), vidta specifika åtgärder för att skydda sina tjänster mot spridning till allmänheten av terrorisminnehåll (artikel 5.2 och 5.3) samt rapportera om de specifika åtgärder som den har vidtagit eller har för avsikt att vidta till den behöriga myndigheten (artikel 5.5). Samma bedömning gör regeringen beträffande bestämmelserna i artikel 7 som innehåller skyldigheter för värdtjänstleverantörer att i sina användarvillkor klart och tydligt ange sin strategi för att åtgärda spridningen av terrorisminnehåll (artikel 7.1) samt i vissa fall offentliggöra en transparenssrapport (artikel 7.2 och 7.3).

Regeringen anser vidare att även bestämmelserna i artikel 10 tillhör samma kategori. Dessa innehåller skyldigheter för värdtjänstleverantörer att inrätta en effektiv och tillgänglig klagomålsmekanism för innehållsleverantörer vars innehåll avlägsnats eller gjorts oåtkomligt (artikel 10.1), att snabbt granska klagomålen och vidta åtgärder om det inte var berättigat att avlägsna innehållet eller göra det oåtkomligt samt att informera klaganden (artikel 10.2). Detsamma gäller bestämmelsen i artikel 15.1 om skyldigheter för värdtjänstleverantörer att utse eller inrätta en kontakt-

punkt för mottagande av avlägsnandeorder på elektronisk väg samt att säkerställa att information om kontaktpunkten offentliggörs.

Slutligen gör regeringen bedömningen att bestämmelserna i artikel 17 är sådana att det vid överträdelse i första hand behövs ett handlingsdirigerande verktyg. Bestämmelserna innehåller skyldigheter för värdtjänstleverantörer som inte har sitt huvudsakliga verksamhetsställe i unionen att utse en rättslig företrädare i unionen (artikel 17.1), förse denna med nödvändiga befogenheter och resurser (artikel 17.2) samt att underätta behörig myndighet i den medlemsstat där den rättsliga företrädaren är bosatt eller etablerad om beslutet (artikel 17.4).

Som konstaterats i föregående avsnitt bör kravet på sanktioner för överträdelse av dessa bestämmelser, för att sanktionerna ska bli så effektiva som möjligt, genomföras genom att den behöriga myndigheten ges möjlighet att besluta förelägganden. Den behöriga myndigheten bör alltså få förelägga en värdtjänstleverantör som åsidosätter sina skyldigheter att vidta sådana åtgärder som krävs för att denne ska uppfylla skyldigheterna. Ett sådant föreläggande måste kunna förenas med vite. Det är emellertid inte givet att det alltid är nödvändigt att göra detta. Beroende på vem som är mottagare av föreläggandet och vilken typ av överträdelse det avser kan det i ett inledande skede framstå som obehövt med ett vite. Det bör därför anges att ett föreläggande får förenas med vite och på så vis lämnas till den behöriga myndigheten att avgöra detta. Skulle ett föreläggande utan vite inte följas, har den behöriga myndigheten förstås möjlighet att besluta om ett nytt föreläggande som då kan förenas med vite.

När det gäller utformningen av den aktuella bestämmelsen i TCO-lagen har utredningen föreslagit att det i lagtexten ska anges vilka åtgärder som förelägganden kopplade till respektive artikel kan avse. För att åstadkomma en rimlig och tillgänglig utformning av lagtexten innebär utredningens förslag emellertid att de angivna åtgärderna inte fullt ut återger de skyldigheter som anges i förordningen. En sådan diskrepans är, särskilt utifrån legalitetsaspekter, inte önskvärd. För att undvika detta, utan att samtidigt tynga lagtexten med ordagranna återgivelser av förordningens bitvis otympliga artikeltext, bör bestämmelsen i stället endast innehålla hänvisningar till de relevanta artiklarna.

Som *MPRT* påpekar (och som utvecklas närmare i avsnitt 10.3) kan en leverantör av en videodelningsplattform komma att samtidigt omfattas av skyldigheter att vidta specifika åtgärder enligt artikel 5 i TCO-förordningen och att vidta lämpliga åtgärder enligt 9 a kap. 1 § och 3 § radio- och tv-lagen. I sådana fall kan det potentiellt uppstå situationer då det är möjligt för både den behöriga myndigheten och *MPRT* att utfärda förelägganden avseende sådana åtgärder. Även om det inte finns någon risk för att detta skulle kunna medföra parallella vitesförelägganden avseende samma sak – förelägganden avseende lämpliga åtgärder kan inte förenas med viten (17 kap. 11 a § radio- och tv-lagen) – delar regeringen *MPRT*:s uppfattning att det är lämpligt att *MPRT* och den behöriga myndigheten samordnar sig kring hanteringen av denna typ av frågor.

Det kan slutligen noteras att enligt artikel 18 ska även artikel 5.6 förenas med en sanktion. Artikel 5.6 riktar sig emellertid inte till värdtjänstleverantörer utan till den behöriga myndigheten, som enligt bestämmelsen ska rikta ett föreläggande mot en värdtjänstleverantör som inte uppfyller kraven i artikel 5.2 och 5.3. Det nu lämnade förslaget innebär att sådana

förelägganden kan utfärdas direkt med stöd av artikel 5.2 och 5.3 och dessutom förenas med vite. Som utredningen konstaterat innebär detta att det inte finns behov av någon sanktion som direkt kopplas till artikel 5.6.

7.3.2 Handläggningen av ärenden om vitesföreläggande

Regeringens bedömning: Ett ärende om vitesföreläggande kommer att handläggas enligt lagen om viten, förvaltningslagen och förvaltningsprocesslagen. Det finns inte skäl att frånga den ordningen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna har inte lämnat några synpunkter på bedömningen.

Skälen för regeringens bedömning: Lagen (1985:206) om viten (viteslagen) innehåller bestämmelser om handläggningen av ärenden om vitesförelägganden och gäller enligt 1 § viten som enligt lag eller annan författning får föreläggas av myndigheter, såvida inte annat följer av vad som är särskilt föreskrivet. Bestämmelserna i viteslagen, som bl.a. innebär att frågor om utdömmande av viten prövas av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet, är ändamålsenligt utformade för handläggningen av ärenden om vitesförelägganden enligt TCO-lagen. Med undantag för bestämmandet av vitesbelopp, som behandlas i nästa avsnitt, finns det därför inte skäl att införa några särskilda bestämmelser i TCO-lagen om handläggningen av vitesförelägganden.

Som utredningen konstaterar blir vidare förvaltningslagen (2017:900) och förvaltningsprocesslagen (1971:291) tillämpliga på handläggningen hos den behöriga myndigheten respektive i förvaltningsdomstol. Inte heller i dessa delar finns skäl att införa några särskilda bestämmelser i TCO-lagen.

7.3.3 Vitesbeloppet

Regeringens förslag: När vite föreläggs ska beloppet bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna har inte lämnat några synpunkter på förslaget.

Skälen för regeringens förslag: Enligt 3 § viteslagen ska vite, när det föreläggs, fastställas till ett belopp som med hänsyn till vad som är känt om adressatens ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som är förenat med vitet. Samtidigt innehåller artikel 18.2 i TCO-förordningen en icke-uttömmande uppräkningslista av ett antal omständigheter som medlemsstaterna ska säkerställa att de behöriga myndigheterna beaktar när de bl.a. fastställer nivån på sanktioner enligt förordningen. Det gäller följande omständigheter: 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 tjänstleverantörens samarbete med de behöriga myndigheterna, f) värdtjänstleverantörens

karaktär och storlek, i synnerhet huruvida det är ett mikroföretag, litet eller medelstort företag och g) graden av skuld hos värdtjänstleverantören, med beaktande av de tekniska och organisatoriska åtgärder som den har vidtagit för att följa förordningen.

För att säkerställa att de nämnda omständigheterna i artikel 18.2 beaktas när den behöriga myndigheten fastställer vitesbeloppet behöver det föras in en särskild bestämmelse om detta i TCO-lagen. Bestämmelsen bör utformas på så vis att den inte begränsar den behöriga myndighetens möjligheter att även ta hänsyn till andra omständigheter som kan falla in under 3 § viteslagen.

7.4 Sanktionsavgifter

7.4.1 Den behöriga myndigheten ska kunna besluta om sanktionsavgift

Regeringens förslag: Den behöriga myndigheten ska få besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som åsidosätter sina skyldigheter enligt någon av artiklarna 3.3, 3.6, 4.2, 4.7, 6, 11 och 14.5 i TCO-förordningen.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår att det i lagtexten ska anges vilka skyldigheter som följer av respektive artikel.

Remissinstanserna: *Förvaltningsrätten i Jönköping* påpekar att utredningen inte motiverar varför den gängse ordningen vid beslut om sanktionsavgifter – att ansvarig myndighet ansöker om påförande av sådan avgift hos förvaltningsdomstol – frångås. Enligt *Sveriges advokatsamfund* är det ett synnerligen olämpligt förfarande att det är samma myndighet som både utfärdar sanktioner och utreder brottsmisstankar.

Skälen för regeringens förslag: Som framgår av avsnitt 7.2 innehåller flera av de bestämmelser i TCO-förordningen som enligt artikel 18 ska vara förenade med sanktioner skyldigheter av sådan karaktär att ett åsidosättande bör föranleda en bestraffande sanktion. I dessa fall framstår sanktionsavgifter, som kan förväntas verka både effektivt och avskräckande, som en lämplig sanktionsform.

Detta gäller till att börja med bestämmelserna i artiklarna 3.3, 3.6 och 4.2 som innehåller skyldigheter för värdtjänstleverantörer att avlägsna terrorisminnehåll eller göra det oåtkomligt så snart som möjligt, och i alla händelser inom en timme, från mottagandet av en avlägsnandeorder (artikel 3.3), att utan onödigt dröjsmål informera den behöriga myndigheten om de vidtagna åtgärderna (artikel 3.6) samt motsvarande när avlägsnandeordern utfärdats av en behörig myndighet i en annan medlemsstat (artikel 4.2). Detsamma gäller bestämmelserna i artikel 4.7, som innehåller en skyldighet att återställa innehåll eller åtkomsten till det om en utländsk avlägsnandeorder skulle vara oförenlig med förordningen eller EU:s rättighetsstadga, och artikel 6, som innehåller skyldigheter att bevara innehåll som avlägsnats eller gjorts oåtkomligt om detta är nödvändigt för att beslutet om avlägsnande eller oåtkomlighet ska kunna

prövas eller för förebyggande, förhindrande, upptäckt, utredning eller lagföring av terroristbrott.

Regeringen gör även bedömningen att bestämmelserna i artikel 11 om skyldighet för värdtjänstleverantörer att informera innehållsleverantörer om att terrorisminnehåll avlägsnats eller gjorts oåtkomligt (artikel 11.1) samt skälen för detta (artikel 11.2) är sådana att de bör förenas med möjligheter till sanktionsavgift. Detsamma gäller bestämmelsen i artikel 11.3 om förbud i vissa fall mot att under en viss period lämna information enligt de föregående bestämmelserna.

Slutligen anser regeringen att också bestämmelsen i artikel 14.5 tillhör samma kategori. Enlig denna har värdtjänstleverantörer som får kännedom om terrorisminnehåll som medför ett överhängande hot mot en eller flera personers liv en skyldighet att omgående underrätta brottsbekämpande myndigheter.

Åsidosättanden av nämnda bestämmelser bör alltså kunna leda till beslut om sanktionsavgift. Utredningen har föreslagit att det är den behöriga myndigheten som ska besluta om sådan avgift. Detta är en ordning som ifrågasatts av *Förvaltningsrätten i Jönköping* som menar att den gängse ordningen är att beslut om sanktionsavgifter fattas av förvaltningsdomstol efter ansökan av ansvarig myndighet. Regeringen konstaterar att båda alternativen är vanligt förekommande – som exempel på det förra kan dataskyddsregleringen nämnas, där det inom tillämpningsområdena för både EU:s dataskyddsförordning och brottsdatalagen (2018:1177) är tillsynsmyndigheten som beslutar om samtliga sanktionsavgifter (6 kap. 2 och 3 §§ lagen [2018:218] med kompletterande bestämmelser till EU:s dataskyddsförordning och 6 kap. 6 § brottsdatalagen). Generellt sett anses en tillsynsmyndighet lämpad att besluta om sanktionsavgift när reglerna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. En domstol brukar anses mer lämpad att besluta om sanktionsavgift om det är aktuellt att pröva framför allt subjektiva rekvisit eller andra svårbedömda rekvisit (se t.ex. Brottsdatalag, prop. 2017/18:232 s. 332).

Regleringen i TCO-förordningen är bitvis komplicerad. Detta gäller emellertid inte i någon större utsträckning tillämpningen av de bestämmelser som ska förenas med sanktioner. I dessa fall är det i stället främst fråga om huruvida exempelvis en avlägsnandeorder har följts eller om viss information har lämnats. Huvudregeln är vidare att sanktionsavgiftssystem bygger på strikt ansvar (prop. 2017/18:232 s. 324), dvs. det krävs inte att överträdelse skett uppsåtligt eller av oaktsamhet. Som utredningen framhåller kommer en sådan ordning, som alltså innebär att det inte krävs någon prövning av subjektiva rekvisit, bidra till ett effektivt sanktions-system vid överträdelse av TCO-förordningen. Regeringen håller därför med utredningen om att skyldigheten att betala sanktionsavgift bör bygga på ett strikt ansvar. Även om bestämmandet av sanktionsavgiftens storlek (se avsnitt 7.4.2) kan bli mer komplicerat innebär detta sammantaget att den av utredningen föreslagna ordningen framstår som lämplig, dvs. det bör vara tillsynsmyndigheten som beslutar om sanktionsavgift. Beslutet bör dock få överklagas till allmän förvaltningsdomstol (se kapitel 9). På så sätt tillgodoses rättssäkerhetsaspekterna för den som åläggs sanktionsavgift och på sikt kommer det att kunna bildas domstolspraxis till vägledning för tillsynsmyndighetens beslut.

Sveriges advokatsamfund har i sammanhanget ifrågasatt lämpligheten i att samma myndighet både utfärdar sanktioner och utreder brottsmisstankar. Som utvecklas i avsnitt 7.5 innebär förbudet mot dubbelbestraffning emellertid att det inte kommer att vara aktuellt att rikta ett beslut om sanktionsavgift mot en person som samtidigt är föremål för ett brottmålsförfarande med samma gärning som grund.

När det gäller utformningen av den aktuella bestämmelsen i TCO-lagen har utredningen föreslagit att det i lagtexten ska anges vilka skyldigheter som följer av respektive artikel. På motsvarande sätt som i bestämmelsen om vitesföreläggande innebär utredningens förslag emellertid att de skyldigheter som anges i förordningen inte fullt ut återges i lagtexten. Inte heller här är en sådan diskrepans önskvärd. Även denna bestämmelse bör därför, av samma skäl som i fråga om bestämmelsen om vitesföreläggande, endast innehålla hänvisningar till de relevanta artiklarna.

Att sanktionsavgifterna bygger på strikt ansvar behöver inte anges särskilt i bestämmelsen. Vad som däremot måste framgå är att det inte är obligatoriskt för den behöriga myndigheten att besluta om sanktionsavgift även om det finns förutsättningar för detta, dvs. det ska anges att myndigheten får besluta att ta ut en sanktionsavgift. För att ett sanktionsavgiftssystem som utgår från strikt ansvar inte ska strida mot oskuldspresumtionen i Europakonventionen måste det nämligen finnas möjlighet att avstå från beslut om avgift när det framstår som oskäligt att ta ut en sådan (se t.ex. prop. 2021/22:18 s. 66 f.). Detta kan exempelvis vara fallet när åsidosättandet är mindre allvarligt. Dessutom kan det finnas skäl att avstå från att ta ut sanktionsavgift för att förbudet mot dubbelbestraffning annars skulle förhindra ett brottmålsförfarande (mer om detta i avsnitt 7.5).

7.4.2 Sanktionsavgiftens storlek

Regeringens förslag: Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 5 000 000 kronor eller, vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3 i TCO-förordningen, ett sådant högre belopp som följer av artikel 18.3 i TCO-förordningen.

Sanktionsavgiftens storlek ska bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår en annan utformning av den del av bestämmelsen som avser det förhöjda beloppet enligt artikel 18.3.

Remissinstanserna har inte lämnat några synpunkter på förslaget.

Skälen för regeringens förslag: I sanktionsavgiftsregleringar anges ibland fasta belopp som sanktionsavgift ska tas ut med för olika typer av överträdelser. I andra fall är reglerna utformade på så sätt att sanktionsavgiften ska fastställas till ett belopp inom ett bestämt beloppsintervall eller till en viss procent av årsomsättningen i näringsverksamhet.

Utgångspunkten för utformningen av regleringen i TCO-lagen måste vara att en sanktionsavgift, i enlighet med förordningens krav, ska kunna vara effektiv, proportionerlig och avskräckande för samtliga värdtjänst-

leverantörer, dvs. oavsett om det rör sig om fysiska eller juridiska personer och oavsett om de bedriver en mindre verksamhet med begränsade resurser eller en större verksamhet med mycket stora resurser. Regeringen delar därför utredningens bedömning att regleringen bör utformas på så vis att sanktionsavgiften ska fastställas till ett belopp inom ett bestämt beloppsintervall.

Förutom att värdtjänstleverantörernas ekonomiska förmåga kan skilja sig mycket åt, är dessutom de överträdelser av TCO-förordningen som kan leda till en sanktionsavgift av varierande art och karaktär. Beloppsintervallet bör därför vara förhållandevis stort för att ge den behöriga myndigheten utrymme att göra en nyanserad bedömning av avgiftens storlek i det enskilda fallet. Med hänsyn till detta anser regeringen att utredningens förslag att en sanktionsavgift ska bestämmas till lägst 5 000 kr och högst 5 000 000 kr framstår som välavvägt.

Enligt artikel 18.3 har medlemsstaterna en särskild skyldighet att säkerställa att en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3 – dvs. värdtjänstleverantörernas skyldigheter att avlägsna terrorisminnehåll eller göra terrorisminnehåll oåtkomligt – blir föremål för böter på upp till fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret. För att Sverige ska uppfylla denna skyldighet måste ett undantag göras från beloppsintervallets övre gräns när sanktionsavgift ska beslutas för denna typ av underlåtenhet, så att avgiften då kan bestämmas till ett sådant högre belopp som följer av artikel 18.3.

Som redogjorts för i avsnitt 7.3.3 innehåller artikel 18.2 i TCO-förordningen en uppräknning av ett antal omständigheter som medlemsstaterna ska säkerställa att de behöriga myndigheterna beaktar när de bl.a. fastställer nivån på sanktioner enligt förordningen. För att genomföra artikel 18.2 måste det därför framgå av TCO-lagen att även sanktionsavgiftens storlek ska bestämmas med beaktande av dessa omständigheter.

7.4.3 Förfarandet vid beslut om sanktionsavgift

Regeringens förslag: En sanktionsavgift ska endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Ett beslut om sanktionsavgift ska delges.

Sanktionsavgiften ska betalas till den behöriga myndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning. Sanktionsavgiften tillfaller staten.

En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Utredningens förslag överensstämmer i sak med regeringens. Utredningens förslag innehåller en särskild föreskrift om verkställighet enligt utskönningsbalken och har i vissa delar en annan redaktionell utformning.

Remissinstanserna har inte lämnat några synpunkter på förslaget.

Skälen för regeringens förslag: I och med att den behöriga myndigheten ska besluta om sanktionsavgift kommer förvaltningslagen att gälla för förfarandet. Det behövs dock vissa ytterligare förfarandebestämmelser.

Det bör finnas en tidsgräns för den behöriga myndighetens handläggning och möjligheten att besluta om sanktionsavgift. En sanktionsavgift bör endast få beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

På grund av sanktionsavgiftens ingripande karaktär bör ett beslut om avgift delges den betalningsskyldige enligt delgivningslagen (2010:1932).

TCO-förordningen innehåller inte några bestämmelser om att administrativa sanktioner ska tillfalla EU eller i övrigt om hur verkställighet ska ske. I avsaknad av en sådan reglering bör det framgå av TCO-lagen att sanktionsavgiften tillfaller staten. Vidare bör det anges att en sanktionsavgift ska betalas till den behöriga myndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om avgiften inte betalas inom föreskriven tid, bör den behöriga myndigheten vara skyldig att lämna den obetalda avgiften för indrivning. Det krävs inte någon särskild föreskrift för att beslutet om sanktionsavgift ska få verkställas enligt utsökningsbalken (se 3 kap. 1 § utsökningsbalken och prop. 2021/22:206).

I likhet med vad som i allmänhet gäller för sanktionsavgifter bör avgiften preskriberas till den del verkställighet inte har skett inom fem år från det att beslutet fick laga kraft.

7.5 Särskilt om förbudet mot dubbelbestraffning

Regeringens bedömning: Förbudet mot dubbelbestraffning medför inte något behov av särskild reglering i TCO-lagen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Sveriges advokatsamfund* framhåller att utdömande av straffrättslig påföljd och sanktionsavgift har bedömts utgöra dubbelbestraffning. Övriga remissinstanser har inga synpunkter på bedömningen.

Skälen för regeringens bedömning: I det sjunde tilläggsprotokollet till Europakonventionen och i EU:s rättighetsstadga finns bestämmelser om rätten att inte bli lagförd eller straffad två gånger för samma brott (gärning), det s.k. dubbelbestraffningsförbudet. Begreppet straff i den mening som avses i Europakonventionen och EU:s rättighetsstadga anses omfatta både vite och sanktionsavgift (se t.ex. Kompletterande bestämmelser till EU:s cybersäkerhetsakt, prop. 2021/21:186 s. 41).

I TCO-lagen kommer det att uttryckligen regleras i vilka situationer vitesföreläggande respektive sanktionsavgift får beslutas. Som utredningen konstaterar innebär detta att det inte kan uppstå situationer då båda dessa sanktionsformer aktualiseras i anledning av en och samma gärning, dvs. något utrymme för dubbelbestraffning i form av både vite och sanktionsavgift finns inte.

Det kan inte uteslutas att en värdtjänstleverantör, i enlighet med vad utredningen anger, kan komma att bli föremål för en straffrättslig process med anledning av det innehåll som sprids på en värdtjänst. Som *Sveriges advokatsamfund* framhåller skulle i ett sådant fall förbudet mot dubbel-

besträffning innebära att antingen den straffrättsliga processen eller ett sanktionsavgiftsförfarande inte kan drivas vidare, om dessa kan sägas avse samma gärning.

Skulle en sådan situation uppkomma är det enligt regeringen givet att det straffrättsliga förfarandet bör ges företräde. Den behöriga myndigheten bör i ett sådant fall alltså avstå från att besluta om sanktionsavgift, vilket är möjligt redan enligt den i avsnitt 7.4.1 föreslagna bestämmelsen eftersom det enligt den inte kommer att vara obligatoriskt att besluta om sanktionsavgift. Då den skisserade situationen dessutom i praktiken kommer att vara mycket sällsynt, om den alls uppkommer, finns det enligt regeringen inte något behov av att reglera den.

8 Sekretess, uppgiftsutbyte och dataskydd

Den behöriga myndigheten kommer inom ramen för sitt uppdrag att behöva hantera en mängd uppgifter av olika slag, inklusive sådana som kan vara skyddsvärda. Även om det inte finns några bestämmelser i TCO-förordningen som ställer krav på viss sekretess måste det därför övervägas om nuvarande sekretessregler ger ett tillräckligt skydd för dessa uppgifter eller om det finns behov av någon ny sekretessbestämmelse.

TCO-förordningen innehåller i artikel 14 en bestämmelse som innebär att de behöriga myndigheterna i de olika medlemsstaterna ska utbyta information, samordna sig med och samarbeta med varandra och, när så är lämpligt, med Europol. Den behöriga myndigheten kan även komma att behöva samverka med andra nationella myndigheter, framför allt Säkerhetspolisen. Det gäller t.ex. när det finns behov av att inhämta underlag till stöd för bedömningen av om visst innehåll ska anses vara terrorisminnehåll. För att en sådan samverkan ska fungera krävs att uppgiftsutbytet inte hindras av sekretess. Det måste därför även övervägas om det behövs särskilda bestämmelser om uppgiftsutbyte.

Vid handläggningen av ett ärende enligt TCO-förordningen och TCO-lagen (ett ”TCO-ärende”) kommer den behöriga myndigheten dessutom att behöva behandla personuppgifter. Det är därför nödvändigt att också analysera hur reglerna förhåller sig till dataskyddsregleringen.

TCO-lagen lämnar till regeringen att avgöra vilken myndighet som ska vara behörig myndighet. Eftersom reglerna om sekretess, uppgiftsutbyte och dataskydd skiljer sig åt mellan olika myndigheter utgår bedömningarna i detta kapitel emellertid från att det, som i dag, är Polismyndigheten som är behörig myndighet. För det fall regeringen framöver skulle överväga att peka ut någon annan behörig myndighet kan de frågor som behandlas här alltså behöva övervägas på nytt.

8.1 Sekretess hos Polismyndigheten

<p>Regeringens förslag: Sekretess ska gälla hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärende enligt TCO-förordningen och TCO-lagen, om det kan antas att</p>
--

den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. För uppgift i en allmän handling ska sekretessen gälla i högst sjuttio år. Hänvisningen till TCO-förordningen ska vara dynamisk, dvs. avse förordningen enligt den vid varje tidpunkt gällande lydelsen.

Regeringens bedömning: Det behövs inte någon ny sekretessbestämmelse till skydd för Polismyndighetens eller Säkerhetspolisens brottsbekämpande eller brottsförebyggande verksamhet.

Utredningens förslag och bedömning överensstämmer i sak med regeringens. Utredningens förslag har i vissa delar en annan redaktionell utformning.

Remissinstanserna: *Tidningsutgivarna* betonar vikten av att den nya sekretessbestämmelsen utformas med en presumtion för offentlighet. Övriga remissinstanser har inga synpunkter på förslaget eller bedömningen.

Skälen för regeringens förslag och bedömning

Polismyndigheten hanterar uppgifter som kan behöva skyddas

Som utredningen redogör för kan de uppgifter som Polismyndigheten behöver hantera inom ramen för ett TCO-ärende vara av mycket skilda slag. Förutom mer övergripande uppgifter om exempelvis grupperingar, symboler eller uttryck kan ärendena innehålla texter, bilder eller videor som visar allvarlig brottslighet. De kan också innehålla uppgifter om enskildas personliga intressen, t.ex. om fysiska eller juridiska personers kopplingar till en terroristgrupp eller om enskildas eller grupperers religiösa eller politiska övertygelser och aktiviteter. Dessutom kan uppgifter om en värdtjänstleverantörs ekonomiska förhållanden behöva behandlas i ärenden som rör sanktioner.

Uppgifterna kan vidare komma från en rad olika källor. Ett TCO-ärende kan exempelvis inledas efter att uppgifter inkommit från allmänheten eller från Säkerhetspolisen eller andra myndigheter. Under handläggningen av ett ärende kan Polismyndigheten också komma att begära in uppgifter från andra myndigheter med särskild kunskap om terrorism och terrorismrelaterade frågor. Detta kommer framför allt att gälla uppgifter från Säkerhetspolisen, men det kan även bli aktuellt i förhållande till exempelvis Center mot våldsbevakande extremism (CVE) och Totalförsvarets forskningsinstitut (FOI).

Som utredningen konstaterar kan ärenden enligt TCO-förordningen beröra grundläggande frågor om yttrandefrihet och det finns därför ett starkt intresse av långtgående möjligheter till insyn i dessa. Samtidigt kommer, som framgått, de uppgifter som Polismyndigheten kommer att hantera att vara känsliga både med hänsyn till allmänna och enskilda intressen. Regeringen gör därför bedömningen att det måste finnas utrymme att skydda vissa uppgifter som Polismyndigheten hanterat inom ramen för TCO-ärenden med sekretess.

Behovet av skydd för allmänna intressen är uppfyllt genom befintliga bestämmelser

När Polismyndigheten handlägger TCO-ärenden är det fråga om en form av administrativ handläggning, som inte primärt sker för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott (mer om denna bedömning i avsnitt 8.4). Det innebär att de sekretessregler som gäller inom Polismyndighetens brottsförebyggande och brottsbekämpande verksamhet inte blir tillämpliga enbart på den grunden att uppgifter handläggs inom ramen för ett TCO-ärende.

Material som hanteras i ett TCO-ärende kommer emellertid, med hänsyn till TCO-förordningens definition av terrorisminnehåll, regelmässigt att vara sådant att det visar att någon typ av brott har begåtts eller planeras. Som utredningen redogjort för kommer Polismyndigheten i sådana fall även ha anledning att behandla sådant material inom ramen för den brottsförebyggande och brottsbekämpande verksamheten. Bestämmelserna om sekretess i 18 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400) kan då tillämpas på uppgifterna, om det kan antas att syftet med beslutade eller förutsedda åtgärder inom den brottsförebyggande eller brottsbekämpande verksamheten motverkas eller den framtida verksamheten skadas om dessa röjs (1 §) eller om det inte står klart att de kan röjas utan sådana följder (2 §).

De uppgifter som Säkerhetspolisen lämnar till Polismyndigheten i ett TCO-ärende kommer främst att vara hänförliga till Säkerhetspolisens underrättelseverksamhet eller brottsutredningar. Sådana uppgifter kan, under samma förutsättningar som när Polismyndigheten behandlar uppgifter inom ramen för sin brottsförebyggande eller brottsbekämpande verksamhet, skyddas av sekretess vid Säkerhetspolisens med stöd av 18 kap. 1 eller 2 § offentlighets- och sekretesslagen. Sekretessbestämmelsernas utformning innebär dessutom att de, efter överlämnandet till Polismyndigheten, är tillämpliga på uppgifterna även där (se KU 1979/80:37 s. 23).

Mot denna bakgrund gör regeringen bedömningen att det allmännas intresse av att skydda uppgifter i TCO-ärenden som vid ett utlämnande skulle kunna motverka eller skada brottsbekämpande och brottsförebyggande verksamheter har ett tillräckligt skydd genom befintlig reglering. Det behövs därför inte någon ny sekretessbestämmelse till skydd för sådana verksamheter, eller i övrigt till skydd för några allmänna intressen.

Det behövs en ny sekretessbestämmelse till skydd för vissa enskilda intressen

Vissa uppgifter om enskildas personliga och ekonomiska förhållanden som behandlas i ett TCO-ärende är sådana att ett utlämnande kan få negativa konsekvenser för den enskilde. Att Polismyndighetens handläggning av TCO-ärenden inte sker inom ramen för myndighetens brottsförebyggande och brottsbekämpande verksamhet innebär emellertid bl.a. att bestämmelsen i 35 kap. 1 § offentlighets- och sekretesslagen, om sekretess för uppgift om en enskilds personliga och ekonomiska förhållanden, i regel inte kommer att kunna tillämpas på uppgifter i ett sådant ärende. Den sekretessbestämmelse som återstår är då den generella bestämmelsen om sekretess till skydd för uppgift om enskilds personliga förhållanden i

21 kap. 1 § offentlighets- och sekretesslagen, men denna är begränsad till uppgifter som rör en enskilds hälsa eller sexualliv.

Regeringen delar utredningens bedömning att detta skydd inte är tillräckligt. Det behövs därför en ny sekretessbestämmelse som skyddar uppgifter om enskilds personliga och ekonomiska förhållanden hos Polismyndigheten i TCO-ärenden. Den givna utgångspunkten när en sådan bestämmelse utformas är att en begränsning av rätten att ta del av allmänna handlingar inte ska gå utöver vad som är motiverat med hänsyn till de intressen som sekretessen avser att skydda. Dessutom ska sekretessbestämmelser utformas så specifikt som möjligt när det gäller både sekretessens föremål och dess räckvidd, dvs. vilka uppgifter som bestämmelsen skyddar och inom vilken typ av ärenden eller verksamheter som den är tillämplig.

Som framgått kan Polismyndigheten inom ramen för ett TCO-ärende hantera uppgifter av mycket varierande slag, vilket gör det svårt att på förhand avgränsa sekretessens föremål alltför mycket utan att samtidigt riskera att skyddsvärda uppgifter faller utanför bestämmelsens tillämpningsområde. Som utredningen föreslagit bör bestämmelsen därför gälla uppgifter om en enskilds personliga och ekonomiska förhållanden. Sekretessbestämmelsen bör vidare vara tillämplig hos Polismyndigheten i ärenden enligt TCO-förordningen och TCO-lagen. Det är lämpligt att eventuella ändringar i TCO-förordningen får omedelbart genomslag i regleringen. Hänvisningen till förordningen bör därför vara dynamisk, dvs. avse den vid varje tidpunkt gällande lydelsen.

Det vanliga är att sekretessbestämmelser till skydd för uppgifter om enskilda i en verksamhet som avser myndighetsutövning utformas med ett s.k. rakt skaderekvisit, dvs. med en sådan presumtion för att uppgifterna är offentliga som *Tidningsutgivarna* efterfrågar. Något skäl för mer långtgående sekretess än så i den nu aktuella bestämmelsen finns inte. Sekretessen bör därför gälla endast om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

Som utredningen föreslagit bör sekretesstiden bestämmas till högst sjuttio år och sekretessbestämmelsen placeras i anslutning till befintliga sekretessbestämmelser i offentlighets- och sekretesslagen som rör annan verksamhet vid Polismyndigheten. Något skäl att begränsa meddelarfriheten med anledning av den föreslagna sekretessbestämmelsen finns inte.

Slutligen kan det noteras att sekretessen, genom bestämmelsen i 43 kap. 1 § offentlighets- och sekretesslagen, kommer att gälla även vid förvaltningsdomstol när beslut i TCO-ärenden överklagas dit.

8.2 En ny bestämmelse om uppgiftsskyldighet

Regeringens förslag: Säkerhetspolisen ska lämna den behöriga myndigheten de uppgifter som den behöriga myndigheten behöver för att fullgöra sitt uppdrag enligt TCO-förordningen. Säkerhetspolisen har rätt att på begäran ta del av de uppgifter hos den behöriga myndigheten som behövs för att bistå den behöriga myndigheten på detta sätt.

En uppgift ska inte lämnas om det finns en sekretessbestämmelse som är tillämplig på uppgiften och övervägande skäl talar för att det intresse

som sekretessen ska skydda har företrädare framför intresset av att uppgiften lämnas ut.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår en annan utformning av den del av bestämmelsen som avser en avvägning mellan intresset för sekretess och intresset för utlämnande.

Remissinstanserna: *Polismyndigheten* och *Säkerhetspolisen* är positiva till den föreslagna regleringen. Övriga remissinstanser har inga synpunkter på förslaget.

Skälen för regeringens förslag: Enligt artikel 13.2 i TCO-förordningen ska den behöriga myndigheten utföra sina uppgifter utan att efterfråga eller ta emot instruktioner från något annat organ. Detta hindrar inte att Polismyndigheten i sin roll som behörig myndighet kan behöva samverka med andra aktörer för att utbyta och samla in vissa uppgifter, exempelvis underlag som myndigheten anser sig behöva för att bedöma om visst innehåll ska anses vara terrorisminnehåll. Som konstaterats ovan gäller detta framför allt Säkerhetspolisen, men det kan även bli aktuellt att vända sig till exempelvis CVE och FOI.

Om de uppgifter som Polismyndigheten har behov av inte omfattas av sekretess, kan samverkan och utbyte av information ske med stöd av de allmänna samverkansskyldigheterna mellan myndigheter (se bl.a. 8 § förvaltningslagen och 6 kap. 5 § offentlighets- och sekretesslagen). Polismyndigheten kommer emellertid även att ha behov av uppgifter som omfattas av sekretess vid de myndigheter där de förvaras. De uppgifter som är aktuella att hämta in från Säkerhetspolisen kommer t.ex. i många fall att vara hänförliga till myndighetens underrättelseverksamhet och vara sådana att de omfattas av sekretess enligt 18 kap. 2 § och 35 kap. 1 § offentlighets- och sekretesslagen.

Offentlighets- och sekretesslagen innehåller vissa generellt tillämpliga sekretessbrytande bestämmelser, framför allt den s.k. generalklausulen i 10 kap. 27 §. Enligt denna får en sekretessbelagd uppgift lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företrädare framför det intresse som sekretessen ska skydda. Bestämmelsen är emellertid svårtillämpad och kan medföra svåra intresseavvägningar i det enskilda fallet. Det finns därför risk för såväl onödigt restriktiva som alltför extensiva tillämpningar av bestämmelsen. Det finns också en risk för olikheter i tillämpningen. Generalklausulens syfte är vidare att utgöra en ventil för det fall ett utbyte av uppgifter uppenbart behöver ske och lagstiftaren inte har förutsett situationen. Ett rutinmässigt uppgiftsutbyte mellan myndigheter ska följaktligen i regel vara författningsreglerat (jfr prop. 2019/20:123 s. 16 och prop. 1979/80:2 Del A s. 327). Mot den bakgrunden har generalklausulen i ett flertal lagstiftningsärenden som gäller samverkan mellan myndigheter kompletterats med särskilda sekretessbrytande bestämmelser eller uppgiftsskyldigheter som ansetts bättre motsvara behoven av informationsutbyte.

Samverkan mellan Polismyndigheten och Säkerhetspolisen kommer att ske regelbundet och i vissa fall vara brådskande. Det är därför inte lämpligt att grunda informationsutbytet mellan dessa myndigheter på generalklausulen. För att underlätta samarbetet och säkerställa att det finns ett tydligt stöd för att lämna ut sekretesskyddade uppgifter bör i stället, med stöd

av 10 kap. 28 § offentlighets- och sekretesslagen, en särskild bestämmelse om informationsutbyte mellan de båda myndigheterna införs i TCO-lagen. Som utredningen föreslagit bör bestämmelsen innebära både att Säkerhetspolisen ska lämna ut de uppgifter som den behöriga myndigheten behöver för att fullgöra sitt uppdrag enligt TCO-förordningen och att Säkerhetspolisen har rätt att på begäran ta del av de uppgifter hos den behöriga myndigheten som behövs för att bistå denna i dess uppdrag.

Den föreslagna bestämmelsen kan inte tillämpas på vissa uppgifter som härrör från internationella avtal. Det finns nämligen i offentlighets- och sekretesslagen särskilda bestämmelser om sådan sekretess, av vilka det framgår att sekretessbrytande bestämmelser som meddelats med stöd av 10 kap. 28 § inte får tillämpas.

Det kan även finnas särskilt känsliga uppgifter av annat slag som omfattas av sekretess vid Säkerhetspolisen och Polismyndigheten. Det är inte givet att utlämnande av sådana uppgifter alltid bör ske med stöd av den nu föreslagna sekretessbrytande bestämmelsen. Av bestämmelsen bör det därför framgå att en uppgift inte ska lämnas om det finns en sekretessbestämmelse som är tillämplig på uppgiften och övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut (jfr 2 § andra stycket lagen [2016:774] om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet och 4 § andra stycket lagen [2022:613] om finansiell information i brottsbekämpningen).

När det gäller Polismyndighetens samverkan med andra myndigheter än Säkerhetspolisen gör regeringen bedömningen att detta kommer att vara aktuellt i väsentligt mindre utsträckning och att ett eventuellt utlämnande av sekretesskyddade uppgifter i dessa fall bör kunna ske med stöd av generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen.

8.3 Informationsutbyte mellan medlemsstaternas behöriga myndigheter

Regeringens bedömning: Den behöriga myndigheten kan utbyta information med behöriga myndigheter i andra medlemsstater med stöd av artikel 14 i TCO-förordningen. Det finns därför inget behov av kompletterande nationella bestämmelser.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna har inte lämnat några synpunkter på bedömningen.

Skälen för regeringens bedömning: Enligt artikel 14 i TCO-förordningen ska de behöriga myndigheterna i de olika medlemsstaterna utbyta information, samordna sig med och samarbeta med varandra och, när så är lämpligt, med Europol, avseende avlägsnandeorder, specifika åtgärder som vidtas enligt artikel 5 och sanktioner som påförs enligt artikel 18. För att uppfylla kraven i artikel 14 kan informationsutbytet behöva omfatta sekretessbelagda uppgifter.

En uppgift som skyddas av sekretess får enligt 8 kap. 3 § 1 offentlighets- och sekretesslagen lämnas ut till en utländsk myndighet eller en mellanfolklig organisation om utlämnandet sker i enlighet med särskild föreskrift

i lag eller förordning. En föreskrift i en EU-förordning är i detta sammanhang att jämställa med en föreskrift i lag eller förordning (se t.ex. prop. 2018/19:38 s. 88). Detta innebär att föreskrivet informationsutbyte kan ske direkt med stöd av artikel 14, varför det saknas behov av kompletterande nationella bestämmelser.

8.4 Förhållandet till dataskyddsregleringen

Regeringens bedömning: TCO-förordningen och TCO-lagen medför inget behov av ändringar i dataskyddsregleringen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Integritetsskyddsmyndigheten* efterlyser en utförligare analys av gränsdragningen mellan dataskyddsförordningen och brottsdatalagen. Myndigheten anser även att det behövs en analys av om det finns behov av särskilda bestämmelser till skydd för de personer vars personuppgifter kan komma att behandlas i TCO-ärenden. Övriga remissinstanser har inga synpunkter på bedömningen.

Skälen för regeringens bedömning

Tillämpligt regelverk

När Polismyndigheten i sin roll som behörig myndighet handlägger TCO-ärenden behöver den behandla personuppgifter. Dessa kan finnas i det innehåll som är föremål för granskning, men även i exempelvis en anmälan om terrorisminnehåll eller i sådant material som myndigheten hämtar in för att kunna bedöma om det är fråga om terrorisminnehåll eller inte. Myndigheten kan också behöva behandla personuppgifter som inte berör det tänkbara terrorisminnehållet i sig utan som avser berörda innehållsleverantörer och värdtjänstleverantörer, de senare inte minst i ärenden om vitesföreläggande och sanktionsavgift.

För Polismyndighetens personuppgiftsbehandling gäller antingen EU:s dataskyddsförordning, med den tillhörande lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen), eller brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag). Avgörande för vilket regelverk som blir tillämpligt är, såvitt nu är relevant, om behandlingen sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, eller utreda eller lagföra brott eller verkställa straffrättsliga påföljder (artikel 2.2 d i dataskyddsförordningen och 1 kap. 2 § brottsdatalagen). Är så fallet ska brottsdatalagen tillämpas, annars dataskyddsförordningen.

En stor del av den behöriga myndighetens uppgifter enligt TCO-förordningen och TCO-lagen har en uppenbart administrativ karaktär. Det handlar t.ex. om att kontrollera värdtjänstleverantörers användarvillkor (artikel 7.1) eller att värdtjänstleverantörer har utsett eller inrättat en kontaktpunkt (artikel 15.1) eller anmält en rättslig företrädare (artikel 17.1). Personuppgiftsbehandling som är nödvändig för utförandet av sådana uppgifter sker inte i brottsförebyggande eller brottsbekämpande syfte.

Som *Integritetsskyddsmyndigheten* påpekar har andra delar av uppgifterna, framför allt utfärdandet av avlägsnandeordrar, ett närmare samband med Polismyndighetens brottsförebyggande och brottsbekämpande verksamhet. Även om det innehåll som en avlägsnandeorder avser kan vara olagligt, så handlar det emellertid också i dessa delar om en form av administrativt förfarande som inte sträcker sig längre än att säkerställa att det aktuella innehållet avlägsnas. Förfarandet riktar sig dessutom mot värdtjänstleverantörer, dvs. aktörer som i regel inte ansvarar straffrättsligt för det innehåll som sprids på tjänsten. Regeringen delar därför utredningens bedömning att Polismyndighetens personuppgiftsbehandling inte heller i dessa delar kan anses ske primärt i brottsförebyggande eller brottsbekämpande syfte, även om effekterna i förlängningen kan bli positiva för det brottsförebyggande och brottsbekämpande arbetet.

Möjligheterna att besluta om vitesföreläggande eller sanktionsavgift vid överträdelser av TCO-förordningen syftar till att uppnå efterlevnad av förordningen, inte till att bestraffa begångna brott, och sanktionerna utgör inte straffrättsliga påföljder. Inte heller den personuppgiftsbehandling som Polismyndigheten vidtar i sådana ärenden görs därför i syfte att förebygga eller bekämpa brott i brottsdatalagens mening.

Detta innebär sammantaget att dataskyddsförordningen och dataskyddslagen blir tillämpliga på all behandling av personuppgifter som Polismyndigheten vidtar inom ramen för ett TCO-ärende. En annan sak är att vissa personuppgifter i TCO-ärenden kan härröra från verksamheter vid Polismyndigheten eller Säkerhetspolisen där de behandlas i brottsförebyggande eller brottsbekämpande syfte – i sådana fall måste det finnas rättsliga möjligheter att gå från sådan behandling till behandling enligt dataskyddsförordningen.

Det finns rättsligt stöd för nödvändig personuppgiftsbehandling

Dataskyddsförordningen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund (artikel 6). Den behandling av personuppgifter som myndigheter utför görs huvudsakligen med stöd av de rättsliga grunder som kommer till uttryck i artikel 6.1 c eller e, och som enligt artikel 6.3 ska fastställas i enlighet med unionsrätten eller nationell rätt. Den rättsliga grunden enligt artikel 6.1 c innebär att behandlingen är laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Begreppet omfattar i första hand offentligrättsliga förpliktelser. Av 2 kap. 1 § dataskyddslagen följer att en förpliktelse utgör en rättslig grund för behandling av personuppgifter om förpliktelsen följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Den rättsliga grunden enligt artikel 6.1 e innebär att behandlingen är laglig om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. All verksamhet som en myndighet bedriver, inom ramen för sin befogenhet, anses vara av allmänt intresse (prop. 2017/18:105 s. 56–59). Av 2 kap. 2 § 1 dataskyddslagen följer att en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning utgör en rättslig grund för behandling av personuppgifter.

När Polismyndigheten utför sina uppgifter som behörig myndighet så utför den en uppgift av allmänt intresse som följer av lag eller annan författning, dvs. av TCO-förordningen och TCO-lagen. Dessutom innehåller förordningen och lagen rättsliga förpliktelser som innebär att personuppgifter måste behandlas. Den personuppgiftsbehandling som är nödvändig för att utföra uppgifterna som behörig myndighet har alltså rättslig grund enligt artikel 6.1 e och kan även ha det enligt artikel 6.1 c.

De personuppgifter som behandlas i ett TCO-ärende kan utgöra s.k. känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen, exempelvis uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter eller religiös eller filosofisk övertygelse. Sådana uppgifter får endast behandlas under vissa särskilt angivna förutsättningar, bl.a. om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse (artikel 9.2 g). I förarbetena till dataskyddslagen gör regeringen bedömningen att det är ett viktigt allmänt intresse att myndigheterna kan sköta sitt uppdrag på ett korrekt, rättssäkert och effektivt sätt (prop. 2017/18:105 s. 85). När Polismyndigheten behandlar känsliga personuppgifter som är nödvändiga för att utföra uppdraget som behörig myndighet rör det sig således om en sådan behandling som omfattas av artikel 9.2 g. I 3 kap. 3 § första stycket 2 dataskyddslagen klargörs vidare att känsliga personuppgifter får behandlas av en myndighet med stöd av nämnda artikel om behandlingen är nödvändig för handläggningen av ett ärende. Detta innebär att det finns rättsligt stöd för Polismyndighetens behandling av känsliga personuppgifter i den mån sådana är relevanta för ett TCO-ärende, något som regelmässigt kommer att vara fallet.

Även personuppgifter som rör lagöverträdelser enligt artikel 10 i dataskyddsförordningen kommer att behöva behandlas i TCO-ärenden. Eftersom sådana enligt 3 kap. 8 § första stycket dataskyddslagen får behandlas av myndigheter finns rättsligt stöd också för denna del av Polismyndighetens personuppgiftsbehandling.

Detta betyder att det finns rättsligt stöd för den personuppgiftsbehandling som Polismyndigheten behöver vidta inom ramen för ett TCO-ärende.

Som framgått kommer vissa personuppgifter i TCO-ärenden att härröra från verksamheter vid Polismyndigheten eller Säkerhetspolisen där de behandlas i brottsförebyggande eller brottsbekämpande syfte, dvs. inom tillämpningsområdena för brottsdatalagen respektive lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter (Säkerhetspolisens datalag). Som noterats ovan måste det därför även finnas rättsliga möjligheter att gå från sådan behandling till behandling enligt dataskyddsförordningen.

Enligt 2 kap. 22 § brottsdatalagen ska det, innan uppgifter behandlas för ett ändamål utanför den lagens tillämpningsområde, säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet, såvida skyldighet att lämna uppgifterna inte följer av lag eller förordning. En bedömning enligt 2 kap. 22 § måste alltså göras innan uppgifter kan överlämnas från Polismyndighetens brottsförebyggande och brottsbekämpande verksamheter till den del som handlägger TCO-ärenden. I de fall uppgifterna är sådana att de kan behövas i TCO-ärendet kommer proportionalitetskravet, med hänsyn till vikten av en ändamålsenlig handläggning av sådana ärenden, emellertid i regel att vara uppfyllt.

Det finns därför tillräckliga rättsliga möjligheter till sådana överlämnanden redan enligt befintlig reglering.

När det sedan gäller sådana personuppgifter som behandlas vid Säkerhetspolisen framgår det av 2 kap. 4 § andra stycket Säkerhetspolisens datalag att de får behandlas om det är nödvändigt för att tillhandahålla information till Polismyndigheten, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning. Eftersom sådan skyldighet kommer att följa av den i avsnitt 8.2 föreslagna bestämmelsen om uppgiftsskyldighet för Säkerhetspolisen, finns tillräckliga rättsliga möjligheter även för överlämnande av uppgifter från Säkerhetspolisen.

Det finns inte behov av några kompletterande dataskyddsbestämmelser

För personuppgifter som behandlas vid Polismyndigheten eller Säkerhetspolisen i brottsförebyggande eller brottsbekämpande syfte finns särskilda bestämmelser om exempelvis längsta tid för behandling, särskilda upplysningar och tillgång till uppgifterna i brottsdatalagen och polisens brottsdatalag respektive i Säkerhetspolisens datalag. *Integritetsskyddsmyndigheten*, som påpekar att det kan röra sig om känsliga personuppgifter eller personuppgifter som rör lagöverträdelser, anser att det behövs en analys av om det finns behov av sådana särskilda bestämmelser även till skydd för de personer vars personuppgifter kan komma att behandlas i TCO-ärenden.

Med anledning av detta finns skäl att framhålla att även dataskyddsförordningen innehåller en mängd bestämmelser till skydd för den vars personuppgifter behandlas med stöd av förordningen. Av de allmänna principerna för behandling av personuppgifter i artikel 5 följer bl.a. att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (ändamålsbegränsning), vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering) och inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (s.k. lagringsminimering). Vid behandling av känsliga personuppgifter med stöd av artikel 9.2 g uppställer dataskyddsförordningen även ett krav på lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. En sådan åtgärd är den sökbegränsning som gäller enligt 3 kap. 3 § andra stycket dataskyddslagen. Detsamma gäller den sekretess som föreslås gälla till skydd för uppgifter om en enskilds personliga eller ekonomiska förhållanden i TCO-ärenden (se avsnitt 8.1). Dessa bestämmelser motsvarar visserligen inte i alla delar vad som gäller enligt brottsdatalagen och polisens brottsdatalag respektive enligt Säkerhetspolisens datalag, men innebär enligt regeringen att det finns ett tillräckligt skydd för de enskilda vars personuppgifter kan komma att behandlas i TCO-ärenden. Det finns därför inte behov av några kompletterande dataskyddsbestämmelser.

9 Rätten att överklaga ett beslut enligt TCO-förordningen och TCO-lagen

Regeringens förslag: Den behöriga myndighetens beslut enligt TCO-förordningen och TCO-lagen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *TechSverige* välkomnar att det tydligt pekas ut att besluten ska kunna överklagas till förvaltningsdomstol. Övriga remissinstanser har inga synpunkter på förslaget.

Skälen för regeringens förslag: Enligt artikel 9 i TCO-förordningen ska värdtjänstleverantörer och innehållsleverantörer som träffas av vissa angivna beslut enligt förordningen ha rätt till effektiva rättsmedel. Förordningen överlämnar till medlemsstaterna att utforma dessa.

Den vanliga ordningen är att rätten till ett effektivt rättsmedel mot myndighetsbeslut uppnås genom möjligheten att överklaga ett beslut till allmän förvaltningsdomstol (40 § förvaltningslagen). Detta gäller även beslut som fattas med stöd av en EU-förordning. Det finns inte skäl att frånga denna ordning när det gäller beslut som den behöriga myndigheten fattar enligt TCO-förordningen och TCO-lagen. Detta inkluderar de beslut om administrativa sanktioner, i form av antingen vitesföreläggande eller sanktionsavgift, som den behöriga myndigheten kan fatta. Även om dessa kan kräva vissa bedömningar som angränsar till straffrätten, exempelvis om visst innehåll utgör terrorisminnehåll, är detta inte tillräcklig anledning att frånga den sedvanliga ordningen med överklagande till förvaltningsdomstol.

Regeringen anser att det av tydlighetsskäl bör införas en särskild bestämmelse om överklagande i TCO-lagen. Av denna bör det också framgå att det krävs prövningstillstånd vid överklagande till kammarrätten.

10 Behovet av ändringar i annan lagstiftning

Det finns i svensk lagstiftning redan regler som på olika sätt berör de aktörer som i TCO-förordningen kallas värdtjänstleverantörer, exempelvis genom att de åläggs vissa skyldigheter kopplade till innehållet på tjänsten. Det är därför nödvändigt att närmare analysera hur bestämmelserna i förordningen förhåller sig till vissa befintliga lagar – lagen (1998:112) om ansvar för elektroniska anslagstavlor (BBS-lagen), lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster (e-handelslagen) och radio- och tv-lagen (2010:696) – samt överväga om det finns behov av ändringar i dessa.

10.1 Lagen om ansvar för elektroniska anslagstavlor

Regeringens förslag: Lagen om ansvar för elektroniska anslagstavlor ska inte vara tillämplig på meddelanden som omfattas av TCO-förordningen. Hänvisningen till TCO-förordningen ska vara dynamisk, dvs. avse förordningen enligt den vid varje tidpunkt gällande lydelsen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår även att skyldigheten enligt BBS-lagen att ta bort vissa meddelanden inte längre ska omfatta sådana meddelanden som innehåller offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet.

Remissinstanserna: *Sveriges advokatsamfund* anser att det kan uppfattas som motsägelsefullt och leda till bedömningssvårigheter att lagen å ena sidan inte ska gälla meddelanden som omfattas av TCO-förordningen, å andra sidan innehålla en skyldighet att ta bort meddelanden som utgör brottet offentlig uppmaning. *Tidningsutgivarna* tillstyrker förslaget, men understryker att även meddelanden som inte skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen kan omfattas av undantagen från TCO-förordningens tillämpningsområde. Övriga remissinstanser har inga synpunkter på förslaget.

Skälen för regeringens förslag: BBS-lagen är tillämplig på elektroniska anslagstavlor, dvs. tjänster för elektronisk förmedling av meddelanden. Meddelanden i lagens mening kan vara text, bild, ljud eller information i övrigt (1 §). Den som tillhandahåller en sådan tjänst har bl.a. en skyldighet att ha viss uppsikt över tjänsten (4 §) och att ta bort meddelanden från tjänsten, eller på annat sätt förhindra vidare spridning av dessa, om meddelandets innehåll uppenbart är sådant som avses i vissa angivna brottsbestämmelser (5 § första stycket 1). Ett av de brott som räknas upp är offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet i 7 § terroristbrottslagen (2022:666). Den som uppsåtligen eller av grov oaktsamhet bryter mot kravet i 5 § döms till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år (7 § första stycket). Straffbestämmelsen tillämpas emellertid inte om det för gärningen kan dömas till ansvar enligt brottsbalken, lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk eller terroristbrottslagen (7 § andra stycket).

Som utredningen konstaterar är definitionen av värdtjänstleverantör i TCO-förordningen (se kapitel 4) sådan att en värdtjänstleverantör samtidigt kan vara en tillhandahållare av en elektronisk anslagstavla enligt BBS-lagen. Vidare kan meddelanden på en elektronisk anslagstavla vars innehåll utgör uppmaning till terrorism eller särskilt allvarlig brottslighet också vara terrorisminnehåll enligt TCO-förordningen. Detta innebär att reglerna i både förordningen och BBS-lagen kan komma att träffa samma innehåll.

En sådan konflikt är inte lämplig, inte minst eftersom skyldigheterna i TCO-förordningen att avlägsna terrorisminnehåll respektive i BBS-lagen att ta bort meddelanden från elektroniska anslagstavlor båda är förenade med sanktioner i olika form (sanktionsavgift respektive straffansvar). Avlägsnandeskyldigheten enligt TCO-förordningen måste vara förenad med sanktioner enligt artikel 18 (se kapitel 7). Därför bör det, i enlighet med utredningens förslag, göras ett tillägg i 2 § BBS-lagen som innebär

att den lagen inte är tillämplig på meddelanden som omfattas av TCO-förordningen. Det är lämpligt att eventuella ändringar i TCO-förordningen får omedelbart genomslag i regleringen. Hänvisningen till förordningen bör därför vara dynamisk, dvs. avse den vid varje tidpunkt gällande lydelsen.

Utredningen har även föreslagit att hänvisningen till offentlig uppmaning i 5 § första stycket 1 BBS-lagen bör utgå. Regeringen konstaterar emellertid att det föreslagna tillägget i 2 § i sig är tillräckligt för att undvika en konflikt mellan författningarna, samtidigt som inkluderingen av offentlig uppmaning i 5 § BBS-lagen fortfarande har ett berättigande. BBS-lagen kan nämligen, till skillnad från TCO-förordningen, även tillämpas på privata, icke kommersiella tillhandahållare av elektroniska anslagstavlor. Bestämmelsen i 5 § BBS-lagen kan alltså tillämpas på ett meddelande som innehåller offentlig uppmaning, men som finns på en elektronisk anslagstavla som tillhandahålls av en privat, icke kommersiell aktör och därför inte omfattas av TCO-förordningen. Dessutom är BBS-lagen för närvarande föremål för en bredare översyn genom Utredningen om kompletterande bestämmelser till EU:s förordning om en inre marknad för digitala tjänster (I 2022:02), varför det finns anledning att begränsa de ändringsförslag som lämnas inom ramen för detta lagstiftningsärende. Regeringen anser därför inte att det finns tillräckliga skäl att låta hänvisningen till offentlig uppmaning i 5 § första stycket 1 BBS-lagen utgå.

Sveriges advokatsamfund invänder att detta skulle kunna leda till bedömningssvårigheter. Regeringen konstaterar emellertid att eventuella sådana svårigheter snarast beror på de otydligheter som finns kring vilka aktörer som omfattas av TCO-förordningen. Som konstaterats i avsnitt 5.1 är detta inte något som kan förtydligas genom ändringar i svensk rätt.

10.2 Lagen om elektronisk handel och andra informationssamhällets tjänster

Regeringens bedömning: TCO-förordningen och TCO-lagen medför inget behov av ändringar i lagen om elektronisk handel och andra informationssamhällets tjänster.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna har inte lämnat några synpunkter på bedömningen.

Skälen för regeringens bedömning: 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 (e-handelsdirektivet) har genomförts i svensk rätt genom e-handelslagen. Lagen gäller informationssamhällets tjänster och påbörjande och utövande av verksamhet som rör sådana tjänster (1 § första stycket). En värdtjänstleverantör enligt TCO-förordningen kommer i regel också att vara en tjänstleverantör i e-handelslagens mening (2 §) och därmed även att omfattas av den lagen.

Regleringen i e-handelslagen är till största delen sådan att någon konflikt med TCO-förordningen och TCO-lagen inte uppkommer. Av särskilt

intresse är emellertid bestämmelsen om ansvarsfrihet i vissa fall i 18 § första stycket e-handelslagen. Enligt denna ska, såvitt nu är relevant, en tjänsteleverantör som lagrar information som lämnats av en tjänstemottagare inte på grund av innehållet i informationen vara skyldig att betala sanktionsavgift, under förutsättning att leverantören antingen 1. inte känner till att den olagliga informationen eller verksamheten förekommer eller 2. utan dröjsmål förhindrar vidare spridning av informationen så snart han får sådan kännedom.

TCO-lagen kommer att ge den behöriga myndigheten möjlighet att besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som åsidosätter vissa skyldigheter enligt TCO-förordningen (se avsnitt 7.4.1). Bland annat gäller detta värdtjänstleverantörens skyldigheter enligt artikel 3.3 och 4.2 att avlägsna terrorisminnehåll eller göra det oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av en avlägsnandeorder.

Ett åsidosättande av skyldigheterna enligt artikel 3.3 och 4.2 kan alltså uppkomma först efter det att värdtjänstleverantören har tagit emot en avlägsnandeorder och genom denna fått kännedom om terrorisminnehållet. Det innebär att TCO-lagen inte ger någon möjlighet att besluta om sanktionsavgift i sådana fall då värdtjänstleverantören ännu inte känner till att innehållet förekommer. Eftersom sanktionsavgift inte heller kan beslutas i de fall värdtjänstleverantören avlägsnar terrorisminnehållet eller gör det oåtkomligt så snart som möjligt efter mottagandet av avlägsnandeordern, bör det inte heller vara möjligt att besluta om sanktionsavgift i sådana fall som omfattas av ansvarsfrihet enligt 18 § första stycket 2 e-handelslagen. Detta innebär att bestämmelsen om ansvarsfrihet i 18 § första stycket e-handelslagen inte kommer i konflikt med TCO-förordningen och TCO-lagen.

Det kan noteras att detta kommer att framgå än tydligare när Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) börjar tillämpas den 17 februari 2024. Förordningen ersätter nämligen bl.a. den del av e-handelsdirektivet som genomförts genom 18 § e-handelslagen och av artikel 2.4 c i förordningen framgår uttryckligen att denna inte ska påverka tillämpningen av TCO-förordningen (vilka författningsändringar som detta föranleder utreds för närvarande av Utredningen om kompletterande bestämmelser till EU:s förordning om en inre marknad för digitala tjänster).

Det finns således, varken med hänsyn till ansvarsfrihetsbestämmelsen eller i övrigt, något behov av ändringar i e-handelslagen.

10.3 Radio- och tv-lagen

Regeringens förslag: Det ska föras in en upplysning i radio- och tv-lagen om att även TCO-förordningen och TCO-lagen gäller för leverantörer av videodelningsplattformar.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Myndigheten för press, radio och tv (MPRT)* tillstyrker förslaget, men ifrågasätter om inte TCO-förordningen kan bli tillämplig även på audiovisuella medietjänster. Övriga remissinstanser har inga synpunkter på förslaget.

Skälen för regeringens förslag: 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 (AV-direktivet) har huvudsakligen genomförts i svensk rätt genom radio- och tv-lagen. När AV-direktivets tillämpningsområde 2018 utvidgades till att även omfatta leverantörer av videodelningsplattformar genom Europaparlamentets och rådets direktiv (EU) 2018/1808 av den 14 november 2018 om ändring av direktiv 2010/13/EU om samordning av vissa bestämmelser som fastställs i medlemsstaternas lagar och andra författningar om tillhandahållande av audiovisuella medietjänster, infördes särskilda bestämmelser om sådana i 9 a kap. radio- och tv-lagen. Av artikel 1.5 i TCO-förordningen framgår bl.a. att förordningen inte ska påverka tillämpningen av AV-direktivet och att AV-direktivet ska äga företräde för audiovisuella medietjänster.

Videodelningsplattformar definieras i radio- och tv-lagen som en tjänst där tjänsten eller en väsentlig funktion i den som huvudsakligt syfte har att, med hjälp av elektroniska kommunikationsnät i informations-, underhållnings- eller utbildningssyfte tillhandahålla allmänheten användargenererade videor eller tv-program som leverantören av tjänsten organiserar men inte har redaktionellt ansvar för (3 kap. 1 § 23). En leverantör av en videodelningsplattform har bl.a. en skyldighet att vidta lämpliga åtgärder för att användargenererade videor, tv-program och audiovisuella kommersiella meddelanden på plattformen inte har ett innehåll som avses i vissa angivna brottsbestämmelser (9 a kap. 3 §). Ett av de brott som räknas upp är offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet i 7 § terroristbrottslagen.

Definitionen av videodelningsplattform är så utformad att leverantören av en sådan samtidigt kan vara en värdtjänstleverantör enligt TCO-förordningen. Dessutom kan innehåll på en videodelningsplattform som utgör uppmaning till terrorism eller särskilt allvarlig brottslighet också vara terrorisminnehåll enligt TCO-förordningen. Detta innebär att reglerna i både förordningen och radio- och tv-lagen kan komma att träffa samma innehåll.

Radio- och tv-lagen innehåller inte någon motsvarighet till TCO-förordningens möjlighet att utfärda en avlägsnandeorder. Skyldigheten att vidta lämpliga åtgärder enligt 9 a kap. 3 § radio- och tv-lagen är däremot så närliggande skyldigheten att vidta specifika åtgärder enligt artikel 5 i förordningen att de båda skyldigheterna kan tänkas överlappa varandra. Någon möjlighet att göra undantag i radio- och tv-lagen, motsvarande vad som föreslagits ovan i BBS-lagen, för att undvika detta finns inte – AV-direktivet skulle då inte vara korrekt genomfört. Till skillnad från vad som gäller enligt BBS-lagen är skyldigheten att vidta lämpliga åtgärder i radio- och tv-lagen emellertid inte förenad med någon form av sanktion eller straff. MPRT, som utövar tillsyn över bestämmelserna i 9 a kap. radio- och tv-lagen, får besluta om de förelägganden som behövs i enskilda fall för att en leverantör av en videodelningsplattform ska följa sin skyldighet, men saknar möjlighet att förena detta med vite. Det innebär att det visser-

ligen är tänkbart att både MPRT och den behöriga myndigheten enligt TCO-förordningen beslutar om förelägganden mot en leverantör av en videodelningsplattform att vidta lämpliga respektive specifika åtgärder, men att det endast är det senare föreläggandet som kan vara förenat med vite.

Eftersom ett åsidosättande av skyldigheten att vidta specifika åtgärder enligt TCO-förordningen måste vara förenat med sanktioner enligt artikel 18 (se kapitel 7), är denna utformning av regelverket oundviklig. Med hänsyn till att leverantören av en videodelningsplattform inte riskerar dubbla sanktionsförfaranden är regeringens bedömning vidare att tillämpningen av AV-direktivet inte kan anses påverkas i en sådan situation. Bestämmelsen i artikel 1.5 i TCO-förordningen kommer därför inte heller att hindra en tillämpning av möjligheten till vitesföreläggande med stöd av den förordningen och TCO-lagen.

Detta innebär sammanfattningsvis att för leverantörer av videodelningsplattformar kan både TCO-förordningen och radio- och tv-lagen vara tillämpliga på samma innehåll och ställa delvis överlappande krav. För att tydliggöra förhållandet bör det, som utredningen föreslagit, tas in en upplysning om detta i 9 a kap. radio- och tv-lagen.

MPRT har ifrågasatt om inte TCO-förordningen kan bli tillämplig även på en annan typ av tjänster som omfattas av radio- och tv-lagen, nämligen audiovisuella medietjänster (dvs. tv-sändningar och beställ-tv). Regeringen konstaterar beträffande detta att utformningen av artikel 1.5, där det anges att AV-direktivet ska äga företräde för audiovisuella medietjänster, närmast tyder på att TCO-förordningen inte alls ska tillämpas på sådana tjänster. Som MPRT anger är emellertid skälen till förordningen något annorlunda utformade, och ger visst stöd för att förordningen skulle kunna tillämpas på audiovisuella medietjänster om detta inte står i konflikt med AV-direktivet (se skäl 8).

TCO-förordningen är direkt tillämplig EU-rätt. Huruvida den kan tillämpas på audiovisuella medietjänster – i den mån leverantören av sådana kan falla under förordningens definition av värdtjänsteleverantör och innehållet inte är skyddat av yttrandefrihetsgrundlagen, vilket i regel är fallet – är därför en fråga för rättstillämpningen och ytterst för EU-domstolen. Detta innebär att det inte är lämpligt att i radio- och tv-lagen ta in någon upplysning om hur sådana tjänster förhåller sig till TCO-förordningen, motsvarande den som föreslagits ovan.

11 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Den nya lagen och lagändringarna ska träda i kraft den 1 juli 2023.

En sanktionsavgift enligt TCO-lagen ska endast få beslutas för sådana åsidosättanden av skyldigheter som har skett efter ikraftträdandet.

Utredningens förslag överensstämmer med regeringens i fråga om ikraftträdandedatum. Utredningen föreslår inga övergångsbestämmelser.

Remissinstanserna har inte lämnat några synpunkter på förslaget.

Skälen för regeringens förslag: TCO-förordningen började tillämpas den 7 juni 2022. Den nya TCO-lagen samt övriga lagändringar bör därför träda i kraft så snart som möjligt, vilket bedöms vara den 1 juli 2023.

I regeringsformen finns ett förbud mot retroaktiv strafflagstiftning (2 kap. 10 §). Förbudet omfattar formellt inte administrativa sanktioner som är av straffliknande natur. Enligt förarbetena skulle det emellertid innebära ett kringgående av förbudet att ge retroaktiv verkan åt administrativa sanktioner av uppenbart repressiv, straffliknande karaktär (prop. 1975/76:209 s. 125). En sanktionsavgift enligt TCO-lagen bör därför endast få beslutas för sådana åsidosättanden av skyldigheter som har skett efter ikraftträdandet, vilket bör anges i en övergångsbestämmelse.

Till skillnad från systemet med sanktionsavgifter är möjligheten enligt TCO-lagen att besluta om vitesförelägganden enbart framåtsyttande. Viten som döms ut på grund av sådana förelägganden kan därför endast avse underlåtenheter att vidta åtgärder i tiden efter lagens ikraftträdande. Även i övrigt saknas behov av övergångsbestämmelser.

12 Konsekvenser

Regeringens bedömning: Förslagen förväntas inte leda till några kostnadsökningar som inte kan finansieras inom ramen för befintliga anslag.

Förslagen bör inte innebära några ekonomiska konsekvenser för de företag som är värdtjänstleverantörer enligt TCO-förordningen.

Förslagen kan få positiva effekter för det brottsförebyggande och brottsbekämpande arbetet.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Riksdagens ombudsmän* och *Sveriges advokatsamfund* framhåller att den behöriga myndigheten kommer att behöva göra kvalificerade rättsliga bedömningar på kort tid och att det därför är nödvändigt att säkerställa att myndigheten har den kompetens som krävs för uppgiften. *Polismyndigheten* konstaterar att det är svårt att beräkna omfattningen av myndighetens uppdrag och därmed även av de kostnadsökningar som förslagen medför. *Förvaltningsrätten i Jönköping* påpekar att det inte finns någon uppskattning av hur många nya mål i förvaltningsdomstolarna som förslagen kan komma att leda till och att det därför finns anledning att följa upp måltillströmningen efter en tid.

Skälen för regeringens bedömning

Ekonomiska konsekvenser för det allmänna

Polismyndigheten är sedan tidigare utsedd till behörig myndighet enligt TCO-förordningen och har därmed redan de arbetsuppgifter som följer av förordningen. De förslag som nu läggs fram innebär att Polismyndigheten

även ges möjligheter att besluta om vitesförelägganden och sanktionsavgifter i TCO-ärenden samt utökade möjligheter till informationsinhämtning. Att arbetet som behörig myndighet, inklusive de uppgifter som följer av förslagen i lagrådsremissen, medför ett ökat administrativt arbete och därmed ökade löpande kostnader för Polismyndigheten är givet. Som *Riksdagens ombudsmän* och *Sveriges advokatsamfund* framhållit är det vidare av vikt att det inom Polismyndigheten finns rätt kompetens. Detta kräver utbildningsinsatser och inrättande av en effektiv organisation för handläggning av TCO-ärenden, dvs. vissa ytterligare initiala kostnader.

Som *Polismyndigheten* konstaterar är det svårt att beräkna omfattningen av myndighetens uppdrag som behörig myndighet och därmed även av de kostnadsökningar som följer av TCO-förordningen och de, mer begränsade, som följer av förslagen i denna lagrådsremiss. Detta har bl.a. att göra med osäkerheten kring begreppet värdtjänstleverantör och hur många aktörer detta träffar, men även med en osäkerhet kring hur behöriga myndigheter i andra medlemsstater kommer att förhålla sig till material som värdtjänstleverantörer med huvudsakligt verksamhetsställe eller rättslig företrädare i Sverige ansvarar för. Som utredningen konstaterar finns emellertid skäl att tro att Polismyndigheten i vart fall inte kommer att behöva handlägga några större mängder av gränsöverskridande avlägsnandeordrar.

Liksom utredningen gör regeringen sammantaget, med beaktande av de osäkerhetsfaktorer som finns, bedömningen att kostnadsökningarna för Polismyndigheten inte kan förväntas vara större än att de rymms inom ramen för myndighetens befintliga anslag.

Förslagen om ökade möjligheter till informationsutbyte mellan Polismyndigheten och Säkerhetspolisen kommer att leda till visst merarbete även för Säkerhetspolisen. Detta är emellertid så begränsat att eventuella kostnadsökningar för myndigheten kan hanteras inom befintligt anslag.

Som Förvaltningsrätten i Jönköping påpekar har utredningen inte gjort någon uppskattning av hur många nya mål i förvaltningsdomstolarna som förslagen kan komma att leda till. Regeringen konstaterar emellertid att det inte finns något som talar för annat än att det kommer att röra sig om ett mycket begränsat antal mål per år. Även för förvaltningsdomstolarnas del kan eventuella kostnadsökningar därför hanteras inom befintligt anslag.

Ekonomiska konsekvenser för företag

TCO-förordningen innehåller en rad skyldigheter för de företag som är värdtjänstleverantörer och vars värdtjänster missbrukas för spridning av terrorisminnehåll. Förslagen i lagrådsremissen innebär emellertid endast att åsidosättanden av sådana skyldigheter kan föranleda administrativa sanktioner, i form av antingen vitesföreläggande eller sanktionsavgift. Förslagen medför alltså inte några nya skyldigheter för värdtjänstleverantörer eller i övrigt något som bör innebära ekonomiska konsekvenser för dessa.

Konsekvenser ur ett rättighetsperspektiv

TCO-förordningen och de kompletterande bestämmelserna i TCO-lagen syftar till att motverka spridning av vissa yttranden och annan information.

Förslagen inverkar alltså på yttrande- och informationsfriheten. Som konstaterats i avsnitt 6.2 är regleringen emellertid inte tillämplig på innehåll som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. I samma avsnitt har det dessutom bedömts att regleringen utgör en godtagbar begränsning av yttrande- och informationsfriheten enligt såväl regeringsformen som Europakonventionen och EU:s rättighetsstadga. Den inverkan som förslagen får på yttrande- och informationsfriheten är alltså rimlig i förhållande till de mål som avses uppnås.

Polismyndigheten kommer inom ramen för TCO-ärenden att behöva behandla en mängd uppgifter om enskilda som kan vara känsliga av olika skäl, bl.a. kommer detta att behövas vid tillämpningen av de föreslagna bestämmelserna om sanktioner och uppgiftsutbyten. Det integritetsingrepp som detta innebär är nödvändigt för att uppfylla TCO-förordningens och TCO-lagens bestämmelser och måste enligt regeringen anses godtagbart, inte minst med hänsyn till den sekretessbestämmelse till skydd för enskilda som föreslås i avsnitt 8.1.

Övriga konsekvenser

Förslagen kommer att bidra till att TCO-förordningen får ett mer effektivt genomslag i Sverige. Därmed ökar möjligheterna att uppnå syftet med förordningen, dvs. att motverka spridning av terrorisminnehåll online och på så vis bl.a. minska risken för att enskilda individer radikaliseras, för att potentiella gärningsmän införskaffar instruktioner och för att terrorattentat livesänds och glorifieras på internet. Dessutom kommer sådan information som Polismyndigheten får kännedom om inom ramen för ett TCO-ärende att i vissa fall kunna vidarebefordras till den brottsbekämpande verksamheten inom Polismyndigheten eller Säkerhetspolisen. Förslagen kan således få positiva effekter både för det brottsförebyggande och det brottsbekämpande arbetet.

13 Författningskommentar

13.1 Förslaget till lag med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online

Lagens innehåll

1 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen).

Paragrafen anger lagens innehåll. Övervägandena finns i avsnitt 5.1.

I paragrafen anges att lagen innehåller bestämmelser som kompletterar TCO-förordningen. Lagen måste därför läsas tillsammans med förordningen.

Termer och uttryck i lagen

2 § Termer och uttryck i denna lag har samma betydelse som i TCO-förordningen.

Paragrafen anger att de termer och uttryck som används i lagen ska förstås på samma sätt som i TCO-förordningen. Övervägandena finns i avsnitt 5.1.

Av paragrafen framgår bl.a. att definitionerna i artikel 2 i TCO-förordningen även gäller vid tillämpningen av lagen.

Behörig myndighet

3 § Den myndighet som regeringen bestämmer är behörig myndighet enligt TCO-förordningen.

Paragrafen anger att regeringen bestämmer behörig myndighet enligt TCO-förordningen. Övervägandena finns i avsnitt 5.2.

Förelägganden

4 § Den behöriga myndigheten får förelägga en värdtjänstleverantör som åsidosätter sina skyldigheter enligt någon av artiklarna 5.1–5.3, 5.5, 7, 10, 15.1 och 17 i TCO-förordningen, i den ursprungliga lydelsen, att vidta sådana åtgärder som krävs för att värdtjänstleverantören ska uppfylla sina skyldigheter.

Ett sådant föreläggande får förenas med vite.

Paragrafen ger den behöriga myndigheten möjlighet att besluta om förelägganden, som får förenas med vite, mot en värdtjänstleverantör som åsidosätter vissa skyldigheter enligt TCO-förordningen. Övervägandena finns i avsnitt 7.3.1.

I *första stycket* ges möjlighet att besluta om förelägganden vid åsidosättanden av de uppräknade skyldigheterna. Det handlar sammanfattningsvis om skyldigheter för värdtjänstleverantörer att

- utforma sina användarvillkor så att de uppfyller kraven i artikel 5.1 och 7.1,
- vidta sådana specifika åtgärder som krävs enligt artikel 5.2 och 5.3,
- rapportera om de specifika åtgärderna enligt artikel 5.5,
- offentliggöra en transparensrapport enligt artikel 7.2 och 7.3,
- inrätta klagomålsmekanismer och granska mottagna klagomål enligt artikel 10,
- utse eller inrätta en kontaktpunkt för mottagande av avlägsnandeordrar enligt artikel 15.1, och
- utse en rättslig företrädare samt förse denna med tillräckliga befogenheter och resurser enligt artikel 17.

Hänvisningen till förordningen är utformad så att den avser förordningen i den ursprungliga lydelsen, s.k. statisk hänvisning.

Enligt *andra stycket* får ett föreläggande förenas med vite. Det är den behöriga myndigheten som avgör om det finns skäl att förena ett föreläggande med vite. Vid bedömningen kan hänsyn tas till exempelvis vem som är mottagare av föreläggandet och vilken typ av överträdelse det avser. Ett föreläggande bör till exempel förenas med vite när det kan befaras att värdtjänstleverantören inte kommer att följa det utfärdade föreläggandet.

Skulle ett föreläggande utan vite inte följas, har den behöriga myndigheten möjlighet att besluta om ett nytt föreläggande som då kan förenas med vite.

När ett föreläggande förenas med vite ska bestämmelserna i lagen (1985:206) om viten (viteslagen) tillämpas, med det tillägg beträffande bestämmandet av vitesbeloppet som följer av 5 §.

5 § När vite föreläggs ska beloppet bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen, i den ursprungliga lydelsen.

Paragrafen anger vissa omständigheter som ska beaktas när vitesbelopp bestäms. Övervägandena finns i avsnitt 7.3.3.

Artikel 18.2 i TCO-förordningen innehåller en uppräkningslista av ett antal omständigheter som medlemsstaterna ska säkerställa att de behöriga myndigheterna beaktar när de bl.a. fastställer nivån på sanktioner enligt förordningen. Dessa omständigheter är följande:

- överträdelsens karaktär, allvar och varaktighet,
- om överträdelsen var avsiktlig eller orsakades av vårdslöshet,
- tidigare överträdelser som värdtjänstleverantören har gjort sig skyldig till,
- värdtjänstleverantörens finansiella styrka,
- graden av tjänstleverantörens samarbete med de behöriga myndigheterna,
- värdtjänstleverantörens karaktär och storlek, i synnerhet huruvida det är ett mikroföretag, litet eller medelstort företag, och
- graden av skuld hos värdtjänstleverantören, med beaktande av de tekniska och organisatoriska åtgärder som den har vidtagit för att följa förordningen.

Av paragrafen följer att den behöriga myndigheten måste beakta dessa omständigheter när vite föreläggs. Uppräkningen är inte uttömmande, vilket innebär att hänsyn även kan tas till andra relevanta omständigheter i enlighet med 3 § viteslagen. Hänvisningen till förordningen är utformad så att den avser förordningen i den ursprungliga lydelsen, s.k. statisk hänvisning.

Sanktionsavgifter

6 § Den behöriga myndigheten får besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som åsidosätter sina skyldigheter enligt någon av artiklarna 3.3, 3.6, 4.2, 4.7, 6, 11 och 14.5 i TCO-förordningen, i den ursprungliga lydelsen.

Paragrafen ger den behöriga myndigheten möjlighet att besluta om uttagande av sanktionsavgift av en värdtjänstleverantör som åsidosätter vissa skyldigheter enligt TCO-förordningen. Övervägandena finns i avsnitt 7.4.1.

Paragrafen innebär att den behöriga myndigheten får besluta att ta ut en sanktionsavgift vid åsidosättanden av de uppräknade skyldigheterna. Det handlar sammanfattningsvis om skyldigheter för värdtjänstleverantörer att

- avlägsna eller göra terrorisminnehåll oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av en avlägsnandeorder enligt artikel 3.3 och 4.2,

- utan onödigt dröjsmål informera den behöriga myndigheten om att terrorisminnehåll har avlägsnats eller gjorts oåtkomligt enligt artikel 3.6,
- omedelbart återställa avlägsnat innehåll eller åtkomsten till det enligt artikel 4.7,
- bevara terrorisminnehåll som avlägsnats eller gjorts oåtkomligt enligt artikel 6,
- informera, eller i vissa fall inte informera, berörd innehållsleverantör om att terrorisminnehåll har avlägsnats eller gjorts oåtkomligt enligt artikel 11, och
- omgående underrätta berörd brottsbekämpande myndighet om terrorisminnehåll som medför ett överhängande hot mot en eller flera personers liv enligt artikel 14.5.

Hänvisningen till förordningen är utformad så att den avser förordningen i den ursprungliga lydelsen, s.k. statisk hänvisning.

Värdtjänstleverantörens ansvar är strikt. Det krävs alltså varken uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut, utan det är tillräckligt att ett åsidosättande har skett. Det är den behöriga myndigheten som avgör om det finns skäl att ta ut en sanktionsavgift. Vid bedömningen måste hänsyn tas till bl.a. oskuldspresumtionen i Europakonventionen. Om det sammantaget framstår som oskäligt att ta ut en avgift, exempelvis för att åsidosättandet är mindre allvarligt, ska någon sådan inte tas ut. Det kan också finnas skäl att avstå från att ta ut sanktionsavgift för att förbudet mot dubbelbestraffning annars skulle förhindra ett brottmålsförfarande mot värdtjänstleverantören.

7 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 5 000 000 kronor eller, vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3 i TCO-förordningen, i den ursprungliga lydelsen, till ett sådant högre belopp som följer av artikel 18.3 i TCO-förordningen, i den ursprungliga lydelsen.

Paragrafen reglerar vilka belopp som sanktionsavgiften ska bestämmas till. Övervägandena finns i avsnitt 7.4.2.

I paragrafen fastställs det lägsta och det högsta beloppet för en sanktionsavgift. När det är fråga om en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3 i TCO-förordningen – dvs. skyldigheterna att avlägsna terrorisminnehåll eller göra terrorisminnehåll oåtkomligt – gäller en särskild regel för bestämmandet av det högsta tillåtna beloppet. Detta får då, i enlighet med vad som anges i artikel 18.3 i förordningen, uppgå till maximalt fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret, om denna summa överstiger 5 000 000 kr. Hänvisningarna till förordningen är utformade så att de avser förordningen i den ursprungliga lydelsen, s.k. statisk hänvisning.

Det är den behöriga myndigheten som beslutar om sanktionsavgiftens storlek. Hur avgiften ska bestämmas i det enskilda fallet regleras i 8 §.

8 § Sanktionsavgiftens storlek ska bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen, i den ursprungliga lydelsen.

Paragrafen reglerar hur sanktionsavgiften ska bestämmas. Övervägandena finns i avsnitt 7.4.2.

Artikel 18.2 i TCO-förordningen innehåller en uppräknning av ett antal omständigheter som medlemsstaterna ska säkerställa att de behöriga myndigheterna beaktar när de bl.a. fastställer nivån på sanktioner enligt förordningen (se kommentaren till 5 §).

Av paragrafen följer att den behöriga myndigheten måste beakta dessa omständigheter när sanktionsavgiftens storlek bestäms. Uppräkningen är inte uttömmande, vilket innebär att hänsyn kan tas även till andra relevanta omständigheter. Hänvisningen till förordningen är utformad så att den avser förordningen i den ursprungliga lydelsen, s.k. statisk hänvisning.

9 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Paragrafen reglerar bl.a. preskriptionstiden för sanktionsavgifter. Övervägandena finns i avsnitt 7.4.3.

Första stycket innebär att kommunikation enligt 25 § förvaltningslagen (2017:900) måste ske inom två år för att en sanktionsavgift ska få beslutas. Tidsfristen räknas från när överträdelsen ägde rum. Bevisbördan för att kommunikation har skett ligger på den behöriga myndigheten.

Andra stycket innebär att ett beslut om sanktionsavgift ska delges den avgiftsskyldige med hjälp av något av de förfaranden för delgivning som regleras i delgivningslagen (2010:1932).

Betalning av sanktionsavgifter

10 § En sanktionsavgift ska betalas till den behöriga myndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom föreskriven tid, ska myndigheten lämna den obetalda avgiften för indrivning enligt lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

Paragrafen reglerar betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 7.4.3.

Om avgiften inte betalas inom den angivna tiden, är den behöriga myndigheten skyldig att lämna den obetalda avgiften för indrivning enligt lagen om indrivning av statliga fordringar m.m. Beslutet om sanktionsavgift utgör en exekutionstitel (3 kap. 1 § första stycket 6 utsökningsbalken). Det innebär att verkställighet enligt utsökningsbalken kan ske utan att det krävs något domstolsavgörande.

11 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Paragrafen reglerar preskription av sanktionsavgifter. Övervägandena finns i avsnitt 7.4.3.

Bestämmelsen innebär att en sanktionsavgift preskriberas om verkställighet inte har skett inom fem år från det att beslutet fick laga kraft. Det som preskriberas är den del av avgiften som inte har drivits in när fem år har gått sedan beslutet fick laga kraft.

Uppgiftsskyldighet

12 § Säkerhetspolisen ska lämna den behöriga myndigheten de uppgifter som den behöriga myndigheten behöver för att fullgöra sitt uppdrag enligt TCO-förordningen.

Säkerhetspolisen har rätt att på begäran ta del av de uppgifter hos den behöriga myndigheten som behövs för att bistå den behöriga myndigheten på det sätt som avses i första stycket.

En uppgift ska inte lämnas om det finns en sekretessbestämmelse som är tillämplig på uppgiften och övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Paragrafen innehåller bestämmelser om uppgiftsskyldighet för Säkerhetspolisen och den behöriga myndigheten. Övervägandena finns i avsnitt 8.2.

Första stycket innehåller en skyldighet för Säkerhetspolisen att lämna ut sådana uppgifter till den behöriga myndigheten som denna behöver för att fullgöra sitt uppdrag enligt TCO-förordningen. Det kan exempelvis röra sig om uppgifter som behövs för att bedöma om ett visst innehåll utgör terrorisminnehåll.

Andra stycket innehåller en motsvarande rätt för Säkerhetspolisen att på begäran ta del av sådana uppgifter hos den behöriga myndigheten som Säkerhetspolisen behöver för att kunna bistå den behöriga myndigheten enligt första stycket. Det kan exempelvis röra sig om sådant innehåll som misstänks utgöra terrorisminnehåll.

Genom uppgiftsskyldigheterna i första och andra styckena blir den sekretessbrytande bestämmelsen i 10 kap. 28 § första stycket offentlighets- och sekretesslagen (2009:400) tillämplig. Bestämmelsen i *tredje stycket* innebär emellertid att en sekretesskyddad uppgift inte ska lämnas om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Säkerhetspolisen och den behöriga myndigheten har alltså ingen absolut skyldighet att lämna ut uppgifter till varandra, utan ska göra en bedömning av om utlämnande ska ske. Det innebär att myndigheterna ska göra en intresseavvägning innan en uppgift lämnas ut. Det krävs inte att det alltid görs en prövning i varje enskilt fall utan en bedömning kan göras utifrån de behov av sekretess som typiskt sett finns för en viss kategori av uppgifter (jfr prop. 1979/80:2 Del A s. 80 f. och 326 f.). Kravet på övervägande skäl ger uttryck för att behovet av att fullgöra uppdraget enligt TCO-förordningen normalt sett har företräde framför andra intressen; det kan sägas råda en presumtion för uppgiftsutlämnande.

Överklagande

13 § Den behöriga myndighetens beslut enligt TCO-förordningen och denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar rätten att överklaga den behöriga myndighetens beslut. Övervägandena finns i kapitel 9.

Första stycket anger att den behöriga myndighetens beslut får överklagas till allmän förvaltningsdomstol. Endast den som beslutet angår får överklaga det, om det har gått honom eller henne emot (42 § förvaltningslagen). Det innebär att en värdtjänstleverantör som mottagit en avlägsnandeorder eller annat beslut som fattats av den behöriga myndigheten med stöd av TCO-förordningen eller TCO-lagen har rätt att överklaga det, liksom en innehållsleverantör vars innehåll berörs av ett sådant beslut.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 juli 2023.
2. En sanktionsavgift enligt 6 § får beslutas endast för sådana åsidosättanden av skyldigheter som har skett efter ikraftträdandet.

Ikraftträdande- och övergångsbestämmelserna behandlas i kapitel 11.

Punkt 1 förskriver när lagen ska träda i kraft.

Punkt 2 innebär att en sanktionsavgift endast kan avse åsidosättanden som har skett efter lagens ikraftträdande.

13.2 Förslaget till lag om ändring i lagen (1998:112) om ansvar för elektroniska anslagstavlor

2 § Lagen gäller dock inte

1. tillhandahållande endast av nät eller andra förbindelser för överföring av meddelanden eller av andra anordningar som krävs för att kunna ta i anspråk ett nät eller annan förbindelse,
2. förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern,
3. tjänster som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen,
4. meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare (elektronisk post), *eller*
5. meddelanden som omfattas av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorism-innehåll online.

Paragrafen innehåller undantag från lagens tillämpningsområde. Övervägandena finns i avsnitt 10.1.

I paragrafen förs en ny *punkt 5* in. Den nya punkten innebär att lagen inte gäller meddelanden som omfattas av TCO-förordningen. Hänvisningen till förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen. För att undantaget ska kunna vara tillämpligt krävs bl.a. att tillhandahållaren av en elektronisk anslagstavla också är en värdtjänstleverantör i TCO-förordningens mening. Det innebär t.ex. att undantaget inte träffar meddelanden på anslagstavlor som tillhandahålls av icke kommersiella aktörer.

13.3 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

35 kap.

TCO-förordningen

23 c § Sekretess gäller hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärende enligt Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och lagen (2023:000) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Paragrafen, som är ny, reglerar sekretessen hos Polismyndigheten i ärenden enligt TCO-förordningen och TCO-lagen. Övervägandena finns i avsnitt 8.1.

I *första stycket* föreskrivs att sekretess gäller hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärende enligt TCO-förordningen och TCO-lagen. Det kan exempelvis vara uppgifter om enskildas kopplingar till en terroristgrupp eller om enskildas religiösa eller politiska övertygelser och aktiviteter. Dessutom kan skyddsvärda uppgifter om en värdtjänstleverantörs ekonomiska förhållanden behöva behandlas i ärenden som rör sanktioner.

Sekretessen gäller om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Det handlar alltså om ett s.k. rakt skaderekvisit, vilket innebär en presumtion för offentlighet.

Hänvisningen till förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

I *andra stycket* anges att sekretessen gäller i högst sjuttio år för uppgift i allmän handling.

13.4 Förslaget till lag om ändring i radio- och tv-lagen (2010:696)

9 a kap.

14 § För leverantörer av videodelningsplattformar gäller även Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och lagen (2023:000) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online.

Paragrafen, som är ny, innehåller en upplysning om att även regleringen i TCO-förordningen och TCO-lagen kan vara tillämplig. Övervägandena finns i avsnitt 10.3.

En leverantör av en videodelningsplattform enligt radio- och tv-lagen kan samtidigt vara en värdtjänstleverantör enligt TCO-förordningen. För

att tydliggöra att regleringen i 9 a kap. inte innehåller en uttömmande reglering av de skyldigheter som en leverantör av en videodelningsplattform kan ha, upplyses i paragrafen om att även TCO-förordningen och TCO-lagen gäller för leverantörer av videodelningsplattformar.

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 marknads funktion bör förbättras genom att rätts-säkerheten 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 medietjänster) (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 förhållbar 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 medie-reglering i enlighet med unionsrätten, inbegripet stadgan. Dessutom bör det gå åt 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 informationssamballets 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 överbelastningsattacker (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 fildelnings-tjänster 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 tillhandahålls 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⁽⁹⁾. 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⁽¹⁰⁾.
- (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 snabb terrorisminnehåll sprids via onlinetjänster bör värdtjänstleverantörerna åläggas en skyldighet att säkerställa att det terrorisminnehåll som anges i avlägsnandeorden avlägsnas eller att det görs oåtkomligt i samtliga medlemsstater inom en timme från mottagandet av avlägsnandeorden. 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 avlägsnandeorden 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 avlägsnandeorden. Om värdtjänstleverantören på grund av force majeure eller faktisk omöjlighet inte kan följa avlägsnandeorden 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 avlägsnandeorden så snart situationen har lösts.

⁽⁹⁾ 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).

⁽¹⁰⁾ 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 akt-samhet 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) Vårdtjänstleverantören 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 vårdtjänstleverantören 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 vårdtjänstleverantören, vårdtjänstleverantörens 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. Vårdtjänstleverantörer 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) Vårdtjänstleverantörernas 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 vårdtjänstleverantörer 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 stadfäst 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 avlägsnandeorden 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 utvärdera 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 anförut 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 anmälningar 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 alltså 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⁽¹⁾. 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.

⁽¹⁾ 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 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 uppmanas 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 överträdelse eller böter vid allvarligare eller systematiska överträdelse. 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 rätts säkerhet bör det i denna förordning anges vilka överträdelse 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 värslöshet eller varit avsiktlig. Medlemsstaterna bör säkerställa att de sanktioner som påförs för överträdelse av denna förordning inte uppmanar 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 iakttä 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
- anstiftar till begäendet 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 förhållande av terroristgränningar, förespråkar begäendet av terroristbrott, och därigenom medför fara för att ett eller flera sådana brott kan begås,
 - 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,
 - 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,
 - 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 begäendet av något av de terroristbrott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541,
 - 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

- 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.
 - 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 avlägsnandeorden utfärdas.
- Första stycket ska inte gälla i vederbörligen motiverade brådskande fall.
- 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 avlägsnandeorden.
 - Behöriga myndigheter ska utfärda avlägsnandeorder med användning av mallen i bilaga I. Avlägsnandeorder ska innehålla följande uppgifter:
 - Identifieringsuppgifter för den behöriga myndighet som utfärdar avlägsnandeorden och den behöriga myndighetens autentisering av avlägsnandeorden.
 - En tillräckligt detaljerad motivering till varför innehållet anses utgöra terrorisminnehåll samt en hänvisning till den relevanta typen av material enligt artikel 2.7.
 - En exakt webbadress (URL) och, vid behov, ytterligare information som gör det möjligt att identifiera terrorisminnehållet.
 - En hänvisning till denna förordning som rättslig grund för avlägsnandeorden.
 - Datum, tidsstämpel och elektronisk signatur för den behöriga myndighet som utfärdar avlägsnandeorden.

- 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 objektiva 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 inletts 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. Vårdtjänstleverantörer 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. Vårdtjänstleverantörer 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. Vårdtjänstleverantörer ska vid behov se över och uppdatera dessa skyddsåtgärder.

AVSNITT III

SKYDDSÅTGÄRDER OCH ANSVARIGHET

Artikel 7

Transparenskrav för vårdtjänstleverantörer

1. Vårdtjänstleverantörer 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 vårdtjänstleverantör som har vidtagit åtgärder för att åtgärda spridningen av terrorisminnehåll eller har ålagt 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 vårdtjänstleverantörens åtgärder för att identifiera och avlägsna terrorisminnehåll eller göra det oåtkomligt.
- b) Information om vårdtjänstleverantörens 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 vårdtjänstleverantören i enlighet med artikel 10 och resultatet av dessa.
- e) Antalet administrativa eller rättsliga prövningsförfaranden som inlett av vårdtjänstleverantören 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 avlägsnandeorden 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 avlägsnandeorden 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 klagorörenden 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 överträdelse 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 överträdelse av bestämmelserna i denna förordning och vidta alla åtgärder som krävs för att säkerställa att de tillämpas. Sådana sanktioner ska vara begränsade till överträdelse 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 sanktionens 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 tjänstleverantörens 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
D.M. SASSOLI
Ordförande

På rådets vägnar
A.P. ZACARIAS
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 begäendet 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 avlägsnandecordern 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 avlägsnandecordern 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 avlägsnandecordern sänds via autentiserade inlämningskanaler som kan garantera att avlägsnandecordern är autentisk.

AVSNITT F: Kontaktuppgifter för uppföljning

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

.....

Kontaktuppgifter till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga 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 avlägsnandeordern

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 värdtjänstleverantören 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:

.....

Sammanfattning av betänkandet EU:s förordning om terrorisminnehåll på internet – kompletteringar och ändringar i svensk rätt (SOU 2022:18)

En ny förordning med 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 (TCO-förordningen) ska tillämpas i Sverige från och med den 7 juni 2022. Förordningen innehåller flera nya rättsliga verktyg för att motverka att terrorisminnehåll sprids till allmänheten på internet.

Den största nyheten är möjligheten att rikta en avlägsnandeorder mot en värdtjänstleverantör med krav på leverantören att avlägsna eller göra visst terrorisminnehåll på internet oåtkomligt inom en timme från mottagandet av avlägsnandeordern. En sådan order riktas således mot den som tillhandahåller den plattform (värdtjänst) där informationen finns och inte mot den som skapat innehållet eller lagt upp det på internet. Det saknar betydelse i vilken medlemsstat värdtjänstleverantören är etablerad. En order kan också, under vissa förutsättningar, riktas mot en värdtjänstleverantör som har sitt huvudsakliga verksamhetsställe utanför EU.

Andra åtgärder i förordningen är mer av tillsynskaraktär och innebär bland annat att en värdtjänstleverantör som vid upprepade tillfällen fått avlägsnandeorder riktade mot sig (i förordningen används begreppet exponerad för terrorisminnehåll) är skyldig att vidta specifika åtgärder för att förhindra att dess värdtjänst missbrukas för spridning av terrorisminnehåll.

Förordningen överlämnar vissa frågor till medlemsstaterna att reglera i nationell rätt. Varje enskild medlemsstat är skyldig att införa ett nationellt sanktionssystem vid överträdelser av förordningen och säkerställa en rätt till effektiva rättsmedel. Utredningen föreslår att sådana bestämmelser samlas i en särskild lag, fortsättningsvis kallad kompletteringslagen.

Behörig myndighet

Medlemsstaterna ska utse en eller flera behöriga myndigheter som ska utföra vissa uppgifter som följer av TCO-förordningen. Den behöriga myndigheten ska till exempel kunna utfärda en avlägsnandeorder mot en värdtjänstleverantör, oavsett var inom unionen denne är etablerad eller registrerad. En annan uppgift är att kontrollera att en värdtjänstleverantör som är exponerad för terrorisminnehåll vidtar specifika åtgärder för att motverka spridning av terrorisminnehåll på dess värdtjänst. Slutligen kan en behörig myndighet besluta om sanktioner mot en värdtjänstleverantör som inte uppfyller skyldigheterna i förordningen. De två senare uppgifterna kan endast riktas mot en värdtjänstleverantör som är etablerad eller registrerad i samma medlemsstat som den behöriga myndigheten. Utredningen har i delbetänkandet *EU:s förordning om terrorisminnehåll*

Värdtjänstleverantör och värdtjänst

TCO-förordningen ställer krav på värdtjänstleverantörer att uppfylla en rad skyldigheter för att motverka spridning av terrorisminnehåll. Utgångspunkten i förordningen är att en värdtjänst i förordningens mening ska *lagra* innehåll på *begäran* av en innehållsleverantör och innehållet ska *spridas till allmänheten*. Den närmare rättsliga tolkningen av begreppet kommer att bli tydligare och preciseras allt eftersom TCO-förordningen börjar tillämpas inom EU.

Innehåll som undantas från TCO-förordningens och kompletteringslagens tillämpningsområde

Visst innehåll som sprids på internet undantas från TCO-förordningens tillämpningsområde. Direkt av förordningen framgår att innehåll som sprids i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller för att öka medvetenheten om terroristverksamhet undantas från tillämpningsområdet. Utredningen har i sin analys av TCO-förordningens förhållande till yttrande- och informationsfriheten i svensk rätt, särskilt skyddet i yttrandefrihetsgrundlagen, bedömt att TCO-förordningen och kompletteringslagen inte heller är tillämpliga i den utsträckning det skulle strida mot de nationella yttrandefrihetsgrundlagarna. Enligt utredningens bedömning påverkar TCO-förordningen därmed inte det grundlagsskyddade området i svensk rätt.

Ett nationellt sanktionssystem

Utredningen har haft i uppdrag att föreslå nationella regler om sanktioner vid överträdelse av vissa bestämmelser i TCO-förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Det är värdtjänstleverantörer – både fysiska och juridiska personer – som kan bli föremål för sanktioner. Utredningens uppfattning är att merparten av värdtjänstleverantörerna kommer att vara juridiska personer.

Utredningen föreslår en möjlighet för den behöriga myndigheten att besluta om administrativa sanktioner. Den behöriga myndigheten ska kunna besluta om vitesföreläggande när syftet med sanktionen är att förbjuda en värdtjänstleverantör att organisera en värdtjänst så att den inte missbrukas för spridning av terrorisminnehåll. Är det i stället fråga om en värdtjänstleverantör som underlåter att till exempel följa en avlägsnandeorder är det mer lämpligt med en sanktion av bestraffande karaktär. I en sådan situation föreslår utredningen att den behöriga myndigheten ska kunna besluta om en sanktionsavgift. En avgift ska tas ut även om överträdelsen inte skett uppsåtligt eller av oaktsamhet, dvs. ett strikt ansvar ska gälla.

När den behöriga myndigheten ska bestämma storleken på såväl vite som en sanktionsavgift ska myndigheten beakta ett antal omständigheter som framgår av TCO-förordningen, bland annat överträdelsens karaktär, allvar och varaktighet och värdtjänstleverantörens finansiella styrka.

Såvitt gäller sanktionsavgifter föreslår utredningen att en avgift ska bestämmas till lägst 5 000 kronor och högst 5 miljoner kronor. Vid en systematisk eller förtgående underlåtenhet att fullgöra skyldigheterna som följer av bestämmelsen om avlägsnandeorder följer det av förordningen att den behöriga myndigheten ska bestämma sanktionsavgiften till högst fyra procent av värdtjänstleverantörens totala omsättning.

Rätten till effektiva rättsmedel

Beslut som den behöriga myndigheten meddelar med stöd av TCO-förordningen eller kompletteringslagen får överklagas till allmän förvaltningsdomstol.

Påverkan på annan nationell lagstiftning

Lagen om (1998:112) om ansvar för elektroniska anslagstavlor (BBS-lagen) kan träffa samma innehåll på internet som omfattas av TCO-förordningen. För att säkerställa att BBS-lagen inte kommer i konflikt med TCO-förordningen föreslår utredningen ändringar i den lagen. Även beträffande radio- och tv-lagen (2010:696) behövs en upplysning om bestämmelserna i TCO-förordningen.

Den myndighet som utses till behörig myndighet enligt TCO-förordningen – enligt utredningens förslag Polismyndigheten – kommer att behöva inhämta information från andra myndigheter kring vad som kan utgöra terrorisminnehåll på internet. Särskilt viktigt bör ett informationsutbyte bli med Säkerhetspolisen. För att underlätta möjligheten för Polismyndigheten och Säkerhetspolisen att utbyta information inom ramen för ett ärende enligt förordningen och kompletteringslagen föreslås en bestämmelse om uppgiftsskyldighet mellan myndigheterna. Uppgiftsskyldigheten betyder att myndigheterna kan utbyta information även om den är skyddad av sekretess vid den utlämnande myndigheten.

Utredningen anser därtill att det finns behov av att föreslå en bestämmelse som skyddar vissa uppgifter i ett TCO-ärende hos Polismyndigheten genom att de omfattas av sekretess.

Förslag till lag (2023:xx) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online, här benämnd TCO-förordningen.

2 § Termer och uttryck i denna lag har samma betydelse som i TCO-förordningen.

Behörig myndighet

3 § Den myndighet regeringen bestämmer är behörig myndighet enligt TCO-förordningen.

Föreläggande

4 § Den behöriga myndigheten får förelägga en värdtjänstleverantör som åsidosätter sina skyldigheter enligt TCO-förordningen, i dess ursprungliga lydelse, att

1. utse eller inrätta en kontaktpunkt för mottagande av avlägsnandeorder enligt artikel 15.1 i TCO-förordningen,

2. utforma sina användarvillkor så att de uppfyller kraven i artikel 5.1 och 7.1 i TCO-förordningen,

3. vidta specifika åtgärder som uppfyller kraven i artikel 5.2 och 5.3 i TCO-förordningen,

4. inrätta klagomålsmekanismer enligt artikel 10.1 i TCO-förordningen,

5. granska klagomål som lämnas in till värdtjänstleverantören enligt artikel 10.2 i TCO-förordningen,

6. lämna in en rapport till den behöriga myndigheten enligt artikel 5.5 i TCO-förordningen,

7. lämna in en transparensrapport enligt artikel 7.2 och 7.3 i TCO-förordningen, och

8. utse en fysisk eller juridisk person till rättslig företrädare enligt kraven i artikel 17 i TCO-förordningen.

Ett föreläggande får förenas med vite.

5 § När vite föreläggs ska beloppet bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen.

Sanktionsavgifter

6 § Den behöriga myndigheten får besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som åsidosätter sina skyldigheter enligt TCO-förordningen, i dess ursprungliga lydelse, genom

1. underlåtenhet att avlägsna terrorisminnehåll eller göra terrorisminnehåll oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern (artikel 3.3 och 4.2 TCO-förordningen),

2. underlåtenhet att utan onödigt dröjsmål informera den behöriga myndigheten att terrorisminnehåll har avlägsnats eller att terrorisminnehåll gjorts oåtkomligt enligt artikel 3.6 i TCO-förordningen,

3. underlåtenhet att enligt artikel 4.7 i TCO-förordningen omedelbart återställa det avlägsnade innehållet eller åtkomsten till det,

4. underlåtenhet att bevara terrorisminnehåll som avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder eller specifika åtgärder enligt artikel 6 i TCO-förordningen,

5. underlåtenhet att informera berörd innehållsleverantör att innehåll avlägsnats eller gjorts oåtkomligt enligt artikel 11.1–11.2 i TCO-förordningen,

6. att lämna ut information i strid med artikel 11.3 i TCO-förordningen, och

7. underlåtenhet att underrätta berörd brottsutredande myndighet om terrorisminnehåll som innebär ett överhängande hot mot en eller flera personers liv (artikel 14.5 TCO-förordningen).

7 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 5 miljoner kronor.

Vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna i artikel 3.3 i TCO-förordningen ska sanktionsavgiften i stället bestämmas enligt artikel 18.3 i TCO-förordningen.

8 § Sanktionsavgiftens storlek ska bestämmas med beaktande av de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen.

9 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Betalning av sanktionsavgifter

10 § En sanktionsavgift ska betalas till den myndighet som regeringen bestämmer enligt 3 § inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Verkställighet får ske enligt utsökningsbalken.

Sanktionsavgiften ska tillfalla staten.

11 § En sanktionsavgift faller bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet fick laga kraft. Bilaga 3

Uppgiftsskyldighet

12 § Säkerhetspolisen ska lämna den behöriga myndigheten de uppgifter som den behöriga myndigheten behöver för att fullgöra sitt uppdrag enligt TCO-förordningen.

Säkerhetspolisen har rätt att på begäran ta del av de uppgifter hos den behöriga myndigheten som behövs för att bistå den behöriga myndigheten på det sätt som avses i första stycket.

Uppgifter ska lämnas om inte särskilda skäl talar mot det.

Överklagande

13 § Den behöriga myndighetens beslut enligt TCO-förordningen och denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 juli 2023.

Förslag till lag om ändring i lagen (1998:112) om ansvar för elektroniska anslagstavlor

Härigenom föreskrivs i fråga om lag (1998:112) om ansvar för elektroniska anslagstavlor att 2 §, 5 § och 7 § ska få följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 §

Lagen gäller dock inte

1. tillhandahållande endast av nät eller andra förbindelser för överföring av meddelanden eller av andra anordningar som krävs för att kunna ta i anspråk ett nät eller annan förbindelse,

2. förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern,

3. tjänster som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller

4. meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare (elektronisk post).

5. meddelanden som omfattas av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.

5 §

Om en användare sänder in ett meddelande till en elektronisk anslagstavla ska den som tillhandahåller tjänsten ta bort meddelandet från tjänsten eller på annat sätt förhindra vidare spridning av meddelandet, om

1. meddelandets innehåll uppenbart är sådant som avses i bestämmelserna om

a) olaga hot i 4 kap. 5 § brottsbalken,

b) olaga integritetsintrång i 4 kap. 6 c § brottsbalken,

c) uppvigling i 16 kap. 5 § brottsbalken,

d) hets mot folkgrupp i 16 kap. 8 § brottsbalken,

e) barnpornografibrott i 16 kap. 10 a § brottsbalken, e) barnpornografibrott i 16 kap. 10 a § brottsbalken, *eller*

f) olaga våldsskildring i 16 kap. 10 c § brottsbalken, eller

g) *offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller*

2. det är uppenbart att användaren har gjort intrång i upphovsrätt eller i rättighet som skyddas genom föreskrift i 5 kap. lagen (1960:729) om

upphovsrätt till litterära och konstnärliga verk genom att sända in Bilaga 3 meddelandet.

För att kunna fullgöra sin skyldighet enligt första stycket har den som tillhandahåller tjänsten rätt att ta del av meddelanden som förekommer i tjänsten.

Skyldigheten enligt första stycket och rätten enligt andra stycket gäller också den som på tillhandahållarens uppdrag har uppsikt över tjänsten.

7 §

Den som uppsåtligen eller av grov oaktsamhet bryter mot 5 § första stycket döms till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år. I ringa fall ska det inte dömas till ansvar.

Första stycket tillämpas inte, om det för gärningen kan dömas till ansvar enligt brottsbalken, lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk *eller lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.*

Första stycket tillämpas inte, om det för gärningen kan dömas till ansvar enligt brottsbalken *eller* lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.

Brott enligt första stycket får i de fall meddelandets innehåll är sådant som avses i bestämmelsen i 4 kap. 6 c § brottsbalken om olaga integritetsintrång åtalas av åklagare endast om målsäganden anger brottet till åtal eller om åtal är påkallat från allmän synpunkt.

Denna lag träder i kraft den 1 juli 2023.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400) att det ska införas en ny paragraf, 35 kap. 23 c §, och närmast före 35 kap. 23 c § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

35 kap.

TCO-förordningen

23 c §

Sekretess gäller hos Polismyndigheten för uppgift i ärende enligt Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen) och lagen (2023:xx) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online till skydd för enskilda personliga eller ekonomiska förhållanden, om det kan antas att en enskild eller någon närstående till denne lider men om uppgiften röjs.

För uppgift i allmän handling gäller sekretess i sjuttio år.

Denna lag träder i kraft den 1 juli 2023.

Förslag till lag om ändring i radio- och tv-lagen (2010:696)

Bilaga 3

Härigenom föreskrivs i fråga om radio- och tv-lagen (2010:696) att det ska införas en ny paragraf, 9 a kap. 14 § av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

9 a kap.

14 §

För leverantörer av videodelningsplattformar gäller även Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och lagen (2023:xx) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online.

Denna lag träder i kraft den 1 juli 2023.

Förteckning över remissinstanserna

Följande remissinstanser har kommit in med yttrande över SOU 2022:18 EU:s förordning om terrorisminnehåll på internet – kompletteringar och ändringar i svensk rätt: Brottsförebyggande rådet, Domstolsverket, Förvaltningsrätten i Jönköping, Integritetsskyddsmyndigheten, Internetstiftelsen, Justitiekanslern, Kammarrätten i Göteborg, Kommerskollegium, Myndigheten för digital förvaltning, Myndigheten för press, radio och tv, Myndigheten för psykologiskt försvar, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen, Riksdagens ombudsmän, Stockholms tingsrätt, Svea hovrätt, Sveriges advokatsamfund, Säkerhetspolisen, TechSverige, Tidningsutgivarna och Totalförsvarets forskningsinstitut.

Följande remissinstans har inte svarat: Sveriges Television AB.