EU:s förordning om terrorisminnehåll på internet

– kompletteringar och ändringar i svensk rätt

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

Stockholm 2022

STATENS OFFENTLIGA UTREDNINGAR

SOU 2022:18

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

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

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

ISBN 978-91-525-0362-1 (tryck)
ISBN 978-91-525-0363-8 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

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

Lagmannen Johan Sjöö förordnades den 30 april 2021 att vara särskild utredare.

Den särskilde utredaren överlämnade den 1 oktober 2021 delbetänkandet *EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet* (SOU 2021:76).

Till sakkunniga förordnades den 1 september 2021 ämnesrådet Filippa Arvas Olsson, Kulturdepartementet, ämnesrådet Henrik Sjölinder, Justitiedepartementet, rättssakkunniga Joanna Hedqvist, Justitiedepartementet och rättssakkunniga Elin Tysklind, Justitiedepartementet. Som experter att biträda utredningen förordnades samma dag internationella chefen Ola Bergström, Post- och telestyrelsen, chefsjuristen Elisabeth Ekstrand, Internetstiftelsen, utredaren Mattias Karlson Jernbäcker, Kommerskollegium, juristen Sofie Klahr, Polismyndigheten, juristen Ingmarie Olsson, Polismyndigheten, och verksjuristen Carl Rundström, Säkerhetspolisen.

Mattias Karlson Jernbäcker entledigades från och med den 2 februari 2022 från sitt uppdrag som expert.

Hovrättsassessorn Lina Molin förordnades som sekreterare i utredningen den 30 april 2021.

Utredningen överlämnar härmed betänkandet *EU:s förordning om terrorisminnehåll på internet – kompletteringar och ändringar i svensk rätt* (SOU 2022:18).

Utredningens uppdrag är med detta slutfört.

Malmö i april 2022

Johan Sjöö

/Lina Molin

Innehåll

Bilagor

Sammanfattning

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 på internet – frågan om behörig myndighet* (SOU 2021:76) föreslagit att Polismyndigheten utses till behörig myndighet för Sveriges räkning.

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 yttrandefrihetsgrund-

lagen, 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 överträdelser 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 förmå 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 uppsåtligen 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 fortgående 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-ordningen. 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.

Summary

A new Regulation with measures to address the dissemination of terrorist content online

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (TCO Regulation) will be applied in Sweden from 7 June 2022. The Regulation contains a number of new legal instruments to counter dissemination of terrorist content to the general public online.

The principal new feature is the possibility to issue a removal order to a hosting service provider, requiring the provider to remove or disable access to specific terrorist content online within one hour of receiving the removal order. Such orders are thus issued to the provider (hosting service) of the platform where the information is found and not to the party who created the content or published it online. The Member State in which the hosting service provider is established is irrelevant. Under certain conditions an order can also be issued to a hosting service provider whose main establishment is outside the EU.

Other measures in the Regulation are supervisory in nature, whereby a hosting service provider that repeatedly receives removal orders (the phrase "exposed to terrorist content" is used in the Regulation) is obliged to take specific measures to prevent misuse of its services for the dissemination of terrorist content.

The Regulation leaves certain issues to the Member States to regulate in national legislation. Each individual Member State is obliged to introduce a national system of penalties for infringements of the Regulation and ensure the right to an effective legal remedy. The Inquiry proposes that such provisions be stipulated in a special act, referred to below as the 'supplementary act'.

Competent authority

The Member States are to appoint an authority or authorities competent to perform certain tasks resulting from the Regulation. The competent authority will, for example, be able to issue removal orders to hosting service providers, irrespective of where they are established or registered in the EU. Another task is to ensure that hosting service providers that are exposed to terrorist content introduce specific measures to address dissemination of terrorist content via their hosting services. Ultimately, a competent authority can impose penalties on hosting service providers that fail to fulfil the obligations in the Regulation. The latter two of these tasks can only be directed at hosting service providers that are established or registered in the same Member State as the competent authority. In its earlier interim report *The EU Regulation on terrorist content online – the question of the competent authority* (SOU 2021:76), the Inquiry proposed that the Swedish Police Authority be appointed the competent authority for Sweden.

Hosting service providers and hosting services

The TCO Regulation sets out requirements on hosting service providers to fulfil a number of obligations to address the dissemination of terrorist content. The starting point in the TCO Regulation is that a hosting service within the meaning of the Regulation *stores* content at the *request* of the content provider and the content is *disseminated to the public*. The legal interpretation of *hosting services* will become clearer and more precise as the TCO Regulation is gradually applied in the EU.

Content that is exempt from the scope of application of the TCO Regulation and the supplementary act

Some content disseminated online is exempt from the scope of application of the TCO Regulation. The Regulation stipulates specifically that content disseminated for educational, journalistic, artistic or research purposes, or for awareness-raising purposes against terrorist activity should be exempt from the scope of application. In its analy-

sis of the TCO Regulation in relation to the freedom of expression and information under Swedish law, particularly the protection regulated in the Fundamental Law on Freedom of Expression, the Inquiry has made the assessment that the TCO Regulation and the supplementary act are not applicable to the extent that this would contravene the national Fundamental Law on Freedom of Expression. Therefore, the Inquiry's assessment is that the TCO Regulation does not affect the constitutionally protected area under Swedish law.

A national system of penalties

The Inquiry was instructed to propose national rules on penalties for infringements of certain provisions in the Regulation. The penalties must be effective, proportionate and dissuasive.

The penalties will apply to hosting service providers – both physical and legal persons. In the Inquiry's estimation, the majority of hosting service providers will be legal persons.

The Inquiry proposes empowering the competent authority to impose administrative penalties. The competent authority will be able to impose conditional financial penalties when the purpose of the penalty is to encourage hosting service providers to configure their hosting services so that they cannot be misused for the dissemination of terrorist content.

If, on the other hand, a hosting service provider fails, for example, to comply with a removal order, a punitive penalty is more appropriate. The Inquiry proposes that the competent authority be able to impose penalty fees in such cases. A fee should be imposed even if the infringement was not committed intentionally or through negligence, i.e. strict liability applies.

When determining the amount of both conditional financial penalties and penalty fees, the competent authority will consider a number of circumstances, as stipulated in the TCO Regulation, including the nature, gravity and duration of the infringement, and the hosting service provider's financial strength.

Regarding penalty fees, the Inquiry proposes that fees of no less than SEK 5 000 and no more than SEK 5 million be imposed. For systematic or continuing failure to fulfil the obligations set out in the provisions on removal orders, the competent authority will impose

a maximum penalty fee of four per cent of the hosting service provider's total turnover.

The right to an effective remedy

Decisions issued by the competent authority based on the TCO Regulation or the supplementary act can be appealed to an administrative court.

Impact on other national legislation

The Act on Responsibility for Electronic Bulletin Boards (1998:112) can apply to the same content online as the TCO Regulation. To ensure that the Act on Responsibility for Electronic Bulletin Boards does not conflict with the TCO Regulation, the Inquiry proposes amendments to the Act. The Radio and Television Act (2010:696) also requires a reference to the provisions in the TCO Regulation.

The authority that is appointed competent authority under the TCO Regulation –the Swedish Police Authority, as per the Inquiry's proposal – will need to obtain information from other authorities concerning what may constitute terrorist content online. An exchange of information with the Swedish Security Service will presumably be especially important. To facilitate exchange of information between the Swedish Police Authority and the Swedish Security Service within the framework of cases under the Regulation and the supplementary act, a provision requiring the disclosure of information between the authorities is proposed. The requirement to disclose information means that the authorities can exchange information even if it is classified as confidential by the disclosing authority.

The Inquiry also considers it necessary to propose a provision whereby certain information in TCO cases handled by the Police Authority can be protected by classifying it as secret.

1 Författningsförslag

1.1 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.

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.

1.2 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 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.

1.3 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 enskilds 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.

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

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.

2 Uppdraget och dess genomförande

2.1 Bakgrund

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 förhärligat 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. Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online är ett resultat av det arbetet. Förordningen kallas fortsättningsvis TCO-förordningen eller förordningen. Förkortningen TCO syftar till förordningens engelska benämning på terrorisminnehåll online, terrorist content online. Förordningen ska tillämpas i alla medlemsstater från och med den 7 juni 2022 och har till syfte att motverka spridningen av terrorisminnehåll på internet och öka den allmänna säkerheten i EU.

TCO-förordningen ställer krav på värdtjänstleverantörer att motverka spridningen av terrorisminnehåll på internet. En av de stora nyheterna är möjligheten för en behörig myndighet i en medlemsstat att utfärda en rättsligt bindande avlägsnandeorder. En värdtjänstleverantör som tar emot en avlägsnandeorder ska inom en timme från mottagandet avlägsna eller göra det aktuella innehållet oåtkomligt i alla medlemsstater. Om en berörd värdtjänstleverantör inte uppfyller skyldigheterna i förordningen kan denne bli föremål för sanktioner.

För en längre redogörelse av bakgrunden till TCO-förordningen och de frivilliga initiativ och rättsliga åtgärder som redan tidigare har

tagits, och håller på att utarbetas, på området hänvisar utredningen till avsnitt 3 i delbetänkandet *EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet* (SOU 2021:76).

2.2 Uppdraget

Den 15 april 2021 beslutade regeringen att ge en särskild utredare i uppdrag att föreslå vilken myndighet som bör pekas ut som behörig myndighet enligt TCO-förordningen för Sveriges räkning. Utredningen fick även i uppdrag att föreslå ändringar och kompletteringar av svensk rätt (dir. 2021:24).

Den första delen av uppdraget, att lämna förslag på en behörig myndighet, redovisades den 1 oktober 2021 i delbetänkandet *EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet* (SOU 2021:76), se mer därom nedan.

Uppdraget i övrigt redovisas genom detta slutbetänkande. I denna del av uppdraget ska utredningen kartlägga vilka sanktioner som skulle kunna aktualiseras vid ett åsidosättande av skyldigheterna i förordningen och lämna förslag på ett nationellt sanktionssystem. Vidare ska utredningen analysera om det finns behov av att ändra befintlig nationell reglering, däribland dataskyddsregleringen och 5 § första stycket och 7 § lagen (1998:112) om ansvar för elektroniska anslagstavlor, och om behov konstateras, lämna förslag till författningsändringar. Sammanfattningsvis ska utredningen i detta slutbetänkande:

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

Utredningens direktiv finns fogade till betänkandet, *bilaga 1*, tillsammans med TCO-förordningen, *bilaga 2*.

2.3 Utredningens arbete

Utredningen påbörjade arbetet i april 2021. Arbetet bestod initialt av kunskapsinhämtning genom till exempel offentliga utredningar, propositioner och publikationer från bland annat Centrum mot våldsbejakande extremism (CVE) vid Brottsförebyggande rådet och Totalförsvarets forskningsinstitut (FOI). Utredningen hade även i det inledande skedet i samma syfte kontakt med representanter för CVE och FOI.

När utredningen inför delbetänkandet övervägde vilken myndighet som bör utses till behörig myndighet var utgångspunkten i direktiven att endast en myndighet bör vara behörig myndighet i Sverige och att utredningen bör överväga om Polismyndigheten eller Säkerhetspolisen bör utses. Utredningen hade därför tidigt i arbetet regelbundna kontakter med företrädare för Polismyndigheten och Säkerhetspolisen. Delbetänkandet överlämnades den 1 oktober 2021 till statsrådet Mikael Damberg. I delbetänkandet föreslog utredningen att Polismyndigheten bör utses till behörig myndighet för Sveriges räkning. Delbetänkandet har remitterats under hösten 2021 och bereds för närvarande inom Regeringskansliet.

Utredningen har i det fortsatta arbetet utgått från hypotesen att Polismyndigheten kommer att utses till behörig myndighet. Arbetet i denna del har bedrivits i nära samarbete med de experter och sakkunniga som förordnades i september 2021.

Utredningen har haft totalt fem utredningssammanträden. Två av dessa har varit fysiska, resterande har genomförts digitalt med anledning av den rådande pandemin. Därutöver har utredningen haft möten och kontakter med de olika experterna och sakkunniga för att diskutera specifika frågor.

Utredningen har även haft kontakt med representanter för bransch- och arbetsgivarorganisationen TechSverige och Myndigheten för press, radio och tv.

Utredningen har deltagit i digitala möten som Europeiska kommissionen anordnat för EU:s medlemsstater med anledning av genomförandet av TCO-förordningen och i digitala möten som anordnats av organisationen Global Internet Forum Counter Terrorism (GIFCT). Därutöver har utredningen haft kontakter med representanter för några enskilda medlemsstater.

3 EU:s förordning om åtgärder mot spridning av terrorisminnehåll på internet

3.1 Inledning

TCO-förordningens övergripande syfte är att säkerställa att den digitala inre marknaden fungerar smidigt i ett öppet och demokratiskt samhälle, genom att motverka att värdtjänster missbrukas för terrorismändamål samt att bidra till den allmänna säkerheten i hela unionen. Den digitala inre marknadens funktion bör förbättras genom att rättssäkerheten ökas för värdtjänstleverantörer och användarnas förtroende stärks för onlinemiljöer samt genom att skyddet för yttrandefriheten förbättras, vilket omfattar friheten att ta emot och sprida information och idéer i ett öppet och demokratiskt samhälle och mediernas frihet och mångfald (artikel 1 och skäl 1).

Det kan inledningsvis konstateras att åtgärderna i TCO-förordningen inte innebär skyldigheter som ska uppfattas som straffrättsliga tvångsmedel av något slag.

3.2 Definitioner och tillämpningsområde

3.2.1 Värdtjänstleverantör

Förordningen innehåller regler för att åtgärda missbruk av värdtjänster som vänder sig till användare i EU, oberoende var i världen värdtjänstleverantören är etablerad. Förordningens definition av värdtjänstleverantör finns i artikel 2.1.

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

Begreppet *tjänst* har samma betydelse som i artikel 1.b i Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (kodifiering). Där framgår att en tjänst omfattar alla informationssamhällets tjänster, det vill säga tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.

En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe inom EU ska utse en fysisk eller juridisk person till *rättslig företrädare* i unionen för mottagande, efterlevnad och verkställighet av avlägsnandeorder eller andra beslut som meddelas av de behöriga myndigheterna i respektive medlemsstat (artikel 17).

Värdtjänstleverantörer som har terrorisminnehåll på sina tjänster är skyldiga att vidta en rad åtgärder som följer av förordningen. En skyldighet är att verkställa avlägsnandeorder och en annan, om leverantören anses exponerad för terrorisminnehåll, är att vidta specifika åtgärder.

Definitionen av värdtjänst och värdtjänstleverantör samt bedömningen av vilka aktörer som kan komma att omfattas av skyldigheterna i förordningen har varit centrala frågor under utredningens arbete. Utredningen återkommer därför till begreppen i avsnitt 4.3.

3.2.2 Innehållsleverantör

En innehållsleverantör är en användare som tillhandahållit den information som lagras och sprids till allmänheten eller har lagrats och spridits till allmänheten av en värdtjänstleverantör (artikel 2.2). En innehållsleverantör vars innehåll avlägsnas eller görs oåtkomligt ska som regel bli informerad om att så skett och har rätt att överklaga

[1] Jfr den engelska versionen: hosting service provider' means a provider of services as defined in point (b) of Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council, consisting of the storage of information provided by and at the request of a content provider.

vissa beslut som meddelas med stöd av TCO-förordningen (artikel 9.2 och 11).

3.2.3 Erbjuda sina tjänster

TCO-förordningen är tillämplig på värdtjänstleverantörer som erbjuder sina tjänster i unionen, oberoende av var deras huvudsakliga verksamhetsställe finns – under förutsättning att de sprider information till allmänheten (artikel 1.2). I skäl 15 och artikel 2.4 framgår att en värdtjänstleverantör anses erbjuda sina tjänster i unionen om den gör 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.

3.2.4 Betydande anknytning till en medlemsstat

Betydande anknytning innebär att en värdtjänstleverantör har anknytning till en eller flera medlemsstater som följer 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 (skäl 16 och artikel 2.5).

Huruvida en verksamhet är riktad till en eller flera medlemsstater avgörs genom en samlad bedömning av relevanta omständigheter, däribland om innehållet på tjänsten är på ett språk eller en valuta som i allmänhet används i den berörda medlemsstaten eller möjligheten att beställa varor eller tjänster från medlemsstaten. Andra omständigheter som talar för att en värdtjänstleverantör har betydande anknytning kan vara att det finns en app tillgänglig i berörd nationell appstore, att lokal marknadsföring eller reklam görs på ett språk som används i den berörda medlemsstaten eller att kundkontakter, såsom kundtjänst, sköts på ett språk som vanligen används i den medlemsstaten. Betydande anknytning antas också 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 av den 12 december 2012 om dom-

stols behörighet och om erkännande och verkställighet av domar på privaträttens område.[2]

Enbart det faktum att en värdtjänstleverantörs webbsida, en e-postadress eller andra kontaktuppgifter är tillgängliga i en eller flera medlemsstater är inte i sig tillräckligt för att leverantören ska anses ha en betydande anknytning till den eller de medlemsstaterna.

3.2.5 Spridning till allmänheten

För att TCO-förordningen ska vara tillämplig på visst innehåll ska innehållet spridas till allmänheten. Det innebär att information görs tillgänglig på begäran av en innehållsleverantör för ett potentiellt obegränsat antal personer (artikel 2.3). Begreppet har betydelse för bedömningen av om en viss värdtjänst omfattas av förordningen och utvecklas närmare i skäl 14. Där framgår att spridning till allmänheten innebär att information görs lätt tillgängligt för användare i allmänhet utan att det krävs någon ytterligare åtgärd från innehållsleverantörens sida, oberoende av om dessa personer verkligen tar del av den aktuella informationen.

Om tillgång till informationen kräver registrering eller tillträde till en grupp av användare bör informationen anses spridd till allmänheten endast när användare automatiskt registreras eller ges tillträde utan att en person beslutar om eller väljer ut vem som ska ges tillgång till informationen. Det innebär att en privat Facebooksida som kräver att en administratör ger en användare tillträde inte omfattas av förordningen. Inte heller e-post och andra privata meddelandetjänster omfattas av TCO-förordningens tillämpningsområde.

3.2.6 Terrorisminnehåll

Förordningen ska motverka spridning av terrorisminnehåll på internet. Terrorisminnehåll kan spridas genom text, bild, ljudupptagning, videos och direktsändning av terroristbrott (skäl 11). Begreppet terrorisminnehåll knyts till den straffrättsliga definitionen av *terroristbrott*

[2] I artikel 17.1 c anges följande; i övriga fall, om avtalet har ingåtts med en person som bedriver kommersiell verksamhet eller yrkesverksamhet i den medlemsstat där konsumenten har hemvist eller, på något sätt, riktar sådan verksamhet till den medlemsstaten eller flera stater, däribland den medlemsstaten, och avtalet faller inom ramen för sådan verksamhet.

i terrorismdirektivet[3]. I artikel 2.6 i TCO-förordningen definieras terrorisminnehåll som material som:

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

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

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

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

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

I terrorismdirektivet framgår definitionen av *terroristbrott* vilken är tillämplig även vid tillämpningen av TCO-förordningen och till vilken det hänvisas i artikel 2.6. I artikel 3 terrorismdirektivet framgår följande.

1. Medlemsstaterna ska vidta nödvändiga åtgärder för att säkerställa att följande uppsåtliga gärningar, vilka till följd av sin art eller sitt sammanhang allvarligt kan skada ett land eller en internationell organisation, definieras som terroristbrott i enlighet med brottsbeskrivningarna i nationell rätt när de begås i något av de syften som anges i punkt 2:

[3] Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (terrorismdirektivet).
[4] Av artikel 4 b) följer: Att delta i en terroristgrupps verksamhet, inbegripet att förse den med information eller materiella resurser eller att bidra med någon form av finansiering av dess verksamhet, med vetskap om att sådant deltagande kommer att bidra till terroristgruppens brottsliga verksamhet.

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

b) Allvarliga angrepp på en persons fysiska integritet.

c) Människorov eller tagande av gisslan.

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

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

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

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

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

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

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

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

a) Injaga allvarlig fruktan hos en befolkning.

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

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

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

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

Andra viktiga faktorer vid bedömningen är om materialet har 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, den s.k. terroristförteckningen[5] (skäl 11).

Visst innehåll undantas från definitionen av terrorisminnehåll. Det handlar om innehåll som sprids till allmänheten i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller i syfte att förhindra eller bekämpa terrorism, inbegripet material som ger uttryck för polemiska eller kontroversiella åsikter inom ramen för den offentliga debatten. Vid bedömningen av om visst material omfattas av undantaget ska särskilt beaktas rätten till yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald samt konstens och vetenskapens frihet. I fall där innehållsleverantören har ett redaktionellt ansvar bör varje beslut om avlägsnande beakta de publicistiska normer som fastställs genom press- och medieregleringen i enlighet med unionsrätten, bland annat EU-stadgan (skäl 12 och artikel 1.3).

[5] Förteckningen beslutas av rådet med stöd av rådets gemensamma ståndpunkt av den 27 december 2001 om tillämpning av särskilda åtgärder i syfte att bekämpa terrorism (2001/931/Gusp) och rådets förordning (EG) nr 2580/2001 av den 27 december 2001 om särskilda restriktiva åtgärder mot vissa personer och enheter i syfte att bekämpa terrorism. Förteckningen ses över minst en gång var sjätte månad.

3.3 Jurisdiktion

En behörig myndighet kan rikta en avlägsnandeorder mot en värdtjänstleverantör oberoende av i vilket land leverantören har sitt huvudsakliga verksamhetsställe, om denne erbjuder sina tjänster i unionen och rekvisiten för utfärdande i övrigt är uppfyllda. Det är fråga om en gränsöverskridande jurisdiktion i artikel 3 som innebär att en behörig myndighet i Sverige kan utfärda en avlägsnandeorder mot en värdtjänstleverantör som till exempel är etablerad i Frankrike eller en värdtjänstleverantör som har registrerat sin rättsliga företrädare i Finland.

Det förhåller sig annorlunda när det är fråga om att påföra en värdtjänstleverantör sanktioner (artikel 18), att besluta om en värdtjänstleverantör är exponerad för terrorisminnehåll eller att utöva tillsyn över en värdtjänstleverantörs specifika åtgärder (artikel 5). I dessa bestämmelser utgår TCO-förordningen i stället från ursprungslandsprincipen. Det innebär att en behörig myndighet i Sverige i detta avseende endast har jurisdiktion över de värdtjänstleverantörer som har sitt huvudsakliga verksamhetsställe i Sverige eller de vars rättsliga företrädare är bosatt eller etablerad här.

Om en värdtjänstleverantör med huvudsakligt verksamhetsställe utanför unionen inte utser en rättslig företrädare har samtliga medlemsstater jurisdiktion. Den medlemsstat som i ett sådant fall utövar sin jurisdiktion ska informera de behöriga myndigheterna i övriga medlemsstater därom (artikel 16).

3.4 Avlägsnandeorder

En avlägsnandeorder innebär en skyldighet för en värdtjänstleverantör att avlägsna terrorisminnehåll eller göra det oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern (artikel 3).

Om myndigheten inte tidigare har utfärdat en avlägsnandeorder mot den aktuella värdtjänstleverantören ska myndigheten informera värdtjänstleverantören om tillämpliga förfaranden och tidsfrister minst tolv timmar innan avlägsnandeordern utfärdas. Kravet på förhandsinformation gäller inte i brådskande fall.

En avlägsnandeorder riktas mot värdtjänstleverantörens huvudsakliga verksamhetsställe eller där den utsedda rättsliga företrädaren

finns och skickas till en utsedd kontaktpunkt. Värdtjänstleverantören ska därefter utan dröjsmål informera utfärdande myndighet när materialet har avlägsnats eller gjorts oåtkomligt. Framkommer det omständigheter av force majeure-karaktär eller en faktisk omöjlighet att avlägsna innehållet ska värdtjänsteleverantören informera den behöriga myndigheten därom.

Om en avlägsnandeorder innehåller uppenbara fel eller inte innehåller tillräcklig information ska värdtjänstleverantören utan onödigt dröjsmål informera myndigheten och be om nödvändiga klargöranden (artikel 3.5–3.8).

En avlägsnandeorder blir slutgiltig – vinner lagakraft – om den inte överklagats inom överklagandefristen eller vid bekräftelse efter ett överklagande (artikel 3.9). Uttrycket ”vid bekräftelse efter ett överklagande” saknar såvitt utredningen känner till motsvarighet i svensk rätt, det får anses motsvara när ett beslut som överklagas sedermera vinner lagakraft.

Innehåll som avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder eller specifika åtgärder ska bevaras i enlighet med kraven i artikel 6. Det har under utredningsarbetet påpekats att TCO-förordningen saknar en bestämmelse som reglerar utlämnande av material för brottsbekämpande ändamål vilket kan komma att innebära problem vid den praktiska tillämpningen av TCO-förordningen.

Särskilt om gränsöverskridande avlägsnandeorder

En gränsöverskridande avlägsnandeorder är en order som utfärdas av en behörig myndighet mot en värdtjänstleverantör som har sitt huvudsakliga verksamhetsställe, eller dess rättsliga företrädare bosatt eller etablerad, i en annan medlemsstat (artikel 4).

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, granska avlägsnandeorden för att fastställa om den på ett allvarligt eller uppenbart sätt är oförenlig med förordningen eller de grundläggande rättigheter och friheter som garanteras i EU-stadgan. Om myndigheten konstaterar oförenlighet ska den, inom samma tid, meddela ett motiverat beslut om detta.

Granskning av en gränsöverskridande avlägsnandeorder kan även komma till stånd genom att värdtjänstleverantören eller innehållsleverantören inom 48 timmar från mottagandet av en avlägsnandeorder, respektive information enligt artikel 11.2, lämnar in en motiverad begäran om granskning till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad. Den behöriga myndigheten ska därefter inom 72 timmar pröva begäran och meddela ett motiverat beslut.

Innan den behöriga myndigheten meddelar ett beslut om oförenlighet ska den informera myndigheten som utfärdat avlägsnandeordern om att den har för avsikt att meddela det aktuella beslutet samt ange skälen till detta (artikel 4.5).

Om den behöriga myndigheten konstaterar oförenlighet gäller inte längre den tidigare avlägsnandeordern. En värdtjänstleverantör som mottar ett beslut om oförenlighet ska omedelbart återställa det avlägsnade innehållet eller åtkomsten till det (artikel 4.6–4.7).

3.5 Specifika åtgärder

En värdtjänstleverantör som är *exponerad* för terrorisminnehåll ska enligt artikel 5 vidta specifika åtgärder för att motverka spridning av sådant innehåll.

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. Vilka andra omständigheter som kan utgöra skäl för att anses exponerad framgår inte av förordningen. Omständigheter som skulle kunna få betydelse är uppgifter som framkommer i en värdtjänstleverantörs transparensrapport.

Om en värdtjänstleverantör anses exponerad för terrorisminnehåll ska värdtjänstleverantören, i tillämpliga fall, i sina användarvillkor inkludera och tillämpa bestämmelser om åtgärder mot missbruk av dess tjänster för spridning av terrorisminnehåll. Det ska göras på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt och, under

alla omständigheter, med hänsyn till användarnas grundläggande rättigheter, särskilt med 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.

En värdtjänstleverantör som är exponerad för terrorisminnehåll ska vidta *specifika åtgärder* för att skydda sina tjänster mot spridning av terrorisminnehåll. Värdtjänstleverantören beslutar självständigt vilka specifika åtgärder som ska vidtas. Förordningen innehåller exempel på åtgärder som värdtjänstleverantören kan använda sig av (artikel 5.2):

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.

De specifika åtgärder som värdtjänstleverantören väljer att tillämpa måste dock på ett effektivt sätt minska graden av exponering för terrorisminnehåll, vara riktade och proportionella, med särskilt beaktande av hur hög graden av exponering för terrorisminnehåll är hos värdtjänstleverantörens tjänster samt värdtjänstleverantörens tekniska och operativa kapacitet och finansiella styrka samt antalet användare av värdtjänstleverantörens tjänster och den mängd innehåll som de tillhandahåller. Åtgärderna måste också 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 och slutligen tillämpas på ett omsorgsfullt och icke-diskriminerande sätt (artikel 5.3).

3.6 Den behöriga myndighetens uppdrag

Varje medlemsstat ska utse en eller flera behöriga myndigheter som ska utföra de uppgifter som följer av artikel 12 TCO-förordningen, nämligen att:

- utfärda avlägsnandeorder,
- granska gränsöverskridande avlägsnandeorder,
- bedöma om en värdtjänstleverantör är exponerad för terrorisminnehåll och övervaka genomförandet av de specifika åtgärder som sådana exponerade värdtjänstleverantörer väljer att vidta, och
- påföra sanktioner.

Medlemsstaterna är skyldiga att säkerställa att deras behöriga myndigheter har de befogenheter och resurser som krävs för att uppnå målen och fullgöra sina skyldigheter enligt förordningen. Medlemsstaterna ska även säkerställa att uppgifterna utförs på ett objektivt och icke-diskriminerande sätt med fullständig respekt för grundläggande rättigheter. En behörig myndighet får inte efterfråga eller ta emot instruktioner från något annat organ när det gäller utförandet av uppgifter enligt (artikel 13.2).

Utredningen har i delbetänkandet *EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet* (SOU 2021:76) föreslagit att regeringen ska utse Polismyndigheten att vara behörig myndighet i Sverige.

3.7 Tillgång till effektiva rättsmedel

Medlemsstaterna ska säkerställa att en värdtjänstleverantör eller en innehållsleverantör som mottar vissa beslut har rätt till effektiva rättsmedel (artikel 9).

Rätten till effektiva rättsmedel innefattar bland annat rätten för värdtjänstleverantörer att bestrida en avlägsnandeorder inför domstolarna i den medlemsstat som utfärdade avlägsnandeordern och rätten att bestrida beslut enligt artikel 4.4 eller artiklarna 5.4, 5.6 eller 5.7 inför domstolarna i den medlemsstat som fattade beslutet.

Medlemsstaterna ska införa effektiva förfaranden för utövandet av de rättigheter som avses i artikel 9. Hur ett sådant förfarande ska

se ut i Sverige är en del av utredningens uppdrag. Utredningens överväganden finns i avsnitt 7.3 och 8.5.13.

3.8 Samarbete och samverkan mellan medlemsstaternas behöriga myndigheter

Förordningen innehåller en särskild artikel om att behöriga myndigheter ska samarbeta och samordna sig bland annat för att undvika dubbelarbete och för att undvika att störa utredningar i andra medlemsstater.

De behöriga myndigheterna ska utbyta information, samordna sig och samarbeta i fråga om övervakning av genomförandet av specifika åtgärder och påförandet av sanktioner.

Det finns även en skyldighet för myndigheterna att skicka in kopior av avlägsnandeorder till Europol (artikel 14.6), att upprätta årliga transparensrapporter om antalet utfärdade avlägsnandeorder och andra beslut som meddelats under året med stöd av förordningen (artikel 8).

Inom ramen för genomförandet av TCO-förordningen arbetar Europol med att ta fram ett särskilt it-system (Plateforme Européen de Retraits de Contenus illicites sur Internet [PERCI]) för att underlätta samarbetet mellan medlemsstaternas behöriga myndigheter. Systemet kommer att utgöra ett centralt verktyg för kommunikation och samarbete i arbetet med avlägsnandeordrar och med frivilliga anmälningar (eng. referrals). Genom PERCI kommer de medlemsstater som väljer att ansluta sig till plattformen att utväxla information om pågående ärenden, beslutade ordrar med mera. På så sätt undviks att flera ordrar utfärdas mot samma innehåll eller att en order utfärdas som påverkar en pågående utredning i en annan medlemsstat. Även kommunikation med värdtjänstleverantörer kan i framtiden komma att ske via PERCI.

3.9 Sanktioner

Slutligen innehåller TCO-förordningen krav på att medlemsstaterna utformar nationella regler om sanktioner vid överträdelser av förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska vidta alla nödvändiga åtgärder för att säkerställa att reglerna tillämpas.

När en behörig myndighet beslutar i ett ärende om påförande av sanktioner ska den beakta alla relevanta omständigheter, däribland 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 värdtjänsteleverantörens 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 denna förordning.

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

Med böter avses här inte enbart böter i straffrättslig mening utan även administrativa sanktioner, så som till exempel sanktionsavgifter.

En del av utredningens uppdrag är att utforma ett nationellt sanktionssystem, se avsnitt 8.

4 Internet – särskilt om begreppen värdtjänst och värdtjänstleverantör

4.1 Inledning

Internet definieras av uppslagsverket Nationalencyklopedin som ett världsomfattande datornät bestående av ett antal regionala och lokala nät som är sammankopplade.[1] Internets användningsområden är i dag många. Användare kan skicka mejl, söka efter information, dela videos och ljudfiler och kommunicera med andra användare via chattfunktioner och sociala medier.

I TCO-förordningen är begreppen *värdtjänst* och *värdtjänstleverantör* centrala för förordningens tillämpning. Detta avsnitt innehåller en kort redogörelse för hur internet är uppbyggt och över några aktörer som är aktiva på internet. Avsnittet redogör även för begreppen värdtjänst och värdtjänstleverantör, hur dessa begrepp definieras i TCO-förordningen men även hur de används i andra rättsakter samt utredningens bedömning av vilka tjänster som skulle kunna rymmas inom förordningens tillämpningsområde.

4.2 Elektroniska kommunikationsnät

Informationssamhällets tjänster[2] erbjuds över öppna eller slutna nät. Det mest kända öppna nätet är internet. Kommunikation över internet sker med kommunikationsprotokollet IP (Internet Protocol) som

[1] Nationalencyklopedin, Internet, www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/internet (hämtad 2021-08-31).
[2] Informationssamhällets tjänster definieras till exempel i 2 § lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster som tjänster som normalt utförs mot ersättning och som tillhandahålls på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.

gör att datorer kan utbyta information med varandra. För att tillhandahålla olika former av tjänster på internet krävs särskilda tillämpningsprotokoll. Det mest kända är www eller World Wide Web.

En *internetleverantör* (eng. Internet Service Provider, ISP) ger en internetanvändare tillgång till internet. När en internetanvändare ska besöka en webbsida kopplar användaren upp sig mot internet genom internetleverantören. Genom leverantörens nätverk och infrastruktur får användaren tillgång till internet. Information som överförs via internet sammanställs, eventuellt mellanlagras, för att slutligen överföras via routrar och serverdatorer.

För att identifiera rätt mottagare av information tilldelas varje dator eller annan utrustning en IP-adress. Varje IP-adress är unik och består av ett antal siffor. En internetanvändare som ska besöka en viss webbsida anger normalt inte en IP-adress utan i stället ett domännamn, till exempel svt.se. Domännamnsystemet förkortas normalt DNS. Det svenska registret med domännamn under toppdomänen .se administreras av Internetstiftelsen med stöd av lagen (2006:24) om nationella toppdomäner för Sverige på internet. Den som registrerar och innehar domännamn kallas domännamnsinnehavare. I Internetstiftelsens register framgår domäninnehavarens namn, e-postadress och postadress.[3]

Andra aktörer på internet är registrarer. De är återförsäljare av domännamn. En registrar kan även vara värdtjänstleverantör, eftersom de ofta erbjuder både domännamn och webbhotell. Registry är den aktör som sköter drift och administration av en toppdomän. Internetstiftelsen är registry för toppdomänen .se.[4]

Den rättsliga regleringen av elektronisk kommunikation tar sin utgångpunkt i lagen (2003:389) om elektronisk kommunikation (LEK).[5] Lagen är teknikneutral och omfattar alla slags elektroniska kommunikationsnät, bland annat internet och elektroniska kommunikationstjänster. Lagen är emellertid inte tillämplig på själva innehållet som överförs i elektroniska kommunikationsnät med hjälp av elektroniska kommunikationstjänster (1 kap. 4 §).

[3] Se även https://internetstiftelsen.se/domaner/vem-tar-ansvar-for-innehall-pa-natet/ (hämtad 2021-12-06).
[4] https://internetstiftelsen.se/domaner/vem-tar-ansvar-for-innehall-pa-natet/ (hämtad 2021-12-01).
[5] EU har antagit direktivet Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning). Sverige har ännu inte implementerat direktivet. I prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation* föreslår regeringen en ny lag om elektronisk kommunikation som ska genomföra direktivet i svensk rätt.

Ett *elektroniskt kommunikationsnät* definieras i lagen som ett system för överföring och, i tillämpliga fall, utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs (1 kap. 7 §). Elektroniska kommunikationsnät kan vara allmänna eller privata. En användare som köper plats på ett webbhotell skapar ett *privat elektroniskt kommunikationsnät*.

Ett *allmänt elektroniskt kommunikationsnät* är till exempel det nät som tillhandahålls av internetoperatörer, dvs. de som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation, till exempel Telia eller Telenor. Den juridiska definitionen av ett allmänt elektroniskt kommunikationsnät följer också av 1 kap. 7 § LEK. Där definieras begreppet som ett elektroniskt kommunikationsnät som helt eller huvudsakligen kan används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stödjer informationsöverföring mellan nätanslutningspunkter.

En *nätanslutningspunkt* är det sätt på vilket en användare av internet normalt ansluter sig till ett allmänt elektroniskt kommunikationsnät, till exempel genom en fiberanslutning (1 kap. 7 §). I nätanslutningspunkten möts det allmänna kommunikationsnätet och abonnentens enskilda nät.

4.3 Värdtjänst och värdtjänstleverantör

4.3.1 Begreppet värdtjänst och värdtjänstleverantör i TCO-förordningen

Begreppet värdtjänstleverantör (eng. *hosting service provider*) har en central roll vid tillämpningen av TCO-förordningen. De skyldigheter som införs genom förordningen är riktade mot värdtjänstleverantörer. Som framgått tidigare definieras begreppet i artikel 2 som en leverantör av tjänster som består i att information som tillhandahållits av en innehållsleverantör lagras på dennes begäran. Med begreppet tjänst avses alla informationssamhällets tjänster, det vill säga tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk

väg och på individuell begäran av en tjänstemottagare.[6] Annorlunda uttryckt handlar det om kommersiella tjänster.

I skälen till TCO-förordningen utvecklas vilka leverantörer som omfattas av förordningens tillämpningsområde. Förordningen omfattar värdtjänstleverantörer som på begäran lagrar och till allmänheten sprider information och material som tillhandahålls av en användare av tjänsten, oavsett om lagringen och spridningen till allmänheten är av rent teknisk, automatisk och passiv karaktär (skäl 13).

Begreppet *lagring* ska förstås som förvaring av data i minnet hos en fysisk eller virtuell server. En värdtjänstleverantör är således normalt en leverantör av informationssamhällets tjänster, till exempel sociala medietjänster, video-, bild- och ljuddelningstjänster, 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 13 och 14).

4.3.2 Begreppet värdtjänst och värdtjänstleverantör i andra rättsakter

Begreppet värdtjänst och värdtjänstleverantör används sedan tidigare i några andra rättsakter från EU. Artikel 14 i e-handelsdirektivet[7] (huvudsakligt införlivat i svensk rätt genom lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster [e-handelslagen]) innehåller en bestämmelse om ansvarsfrihet för värdtjänstleverantörer. En värdtjänstleverantör enligt direktivet är en aktör som levererar någon av informationssamhällets tjänster bestående av lagring av information som tillhandahållits av tjänstemottagare.[8]

---

[6] Begreppet *tjänst* definieras i artikel 1.1. b Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster enligt följande:
1. på distans: tjänster som tillhandahålls utan att parterna är närvarande samtidigt,
2. på elektronisk väg: en tjänst som sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling (inbegripet digital signalkomprimering) och lagring av uppgifter, och som i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel,
3. på individuell begäran av en tjänstemottagare: en tjänst som tillhandahålls genom överföring av uppgifter på individuell begäran.

[7] 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”).

[8] Jfr engelska versionen av artikel 14.1 ”Where an information society service is provided that consists of the storage of information provided by a recipient of the service […].”

Likt TCO-förordningen använder e-handelsdirektivet även begreppet informationssamhällets tjänster. Med utgångspunkt i begreppet ”elektronisk handel” fördes i förarbetena till e-handelslagen ett resonemang kring vilka tjänster som omfattas av begreppet informationssamhällets tjänster:

> Det finns dock inte någon klar eller allmängiltig definition av begreppet elektronisk handel. OECD (Organisation for Economic Co-operation and Development) menar att den engelska motsvarigheten till begreppet e-handel, ”e-commerce”, passar bäst som paraplybegrepp för att täcka in alla former av affärsaktiviteter som sker elektroniskt. I regeringens skrivelse Elektronisk handel (skr. 1997/98:190) anges att begreppet elektronisk handel bör ges en vid definition där alla situationer av utväxlande av affärsinformation via olika former av telekommunikation inbegrips. […] Trots dessa breda definitioner som tagits fram på olika håll verkar det i dagligt tal vara vanligare att tala om elektronisk handel i en något snävare bemärkelse, dvs. om själva handeln av varor och tjänster över Internet. Här används fortsättningsvis elektronisk handel i denna snävare betydelse. Det vidare begreppet informationssamhällets tjänster, som används i bl.a. e-handelsdirektivet (angående definitionen av begreppet, se avsnitt 7.3), inbegriper dock även övriga tjänster som är kopplade till handeln av varor och tjänster över Internet eller andra nät. I begreppet informationssamhällets tjänster ingår därför, förutom själva handeln, en mängd olika tjänster såsom informationstjänster, finansiella tjänster, fastighetsmäklartjänster, webbhotell och söktjänster. En förutsättning för att en tjänst skall omfattas av begreppet är att den tillhandahålls online, dvs. via en förbindelse som möjliggör direkt interaktiv kommunikation.[9]

Begreppet värdtjänstleverantör används även i Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004 (konsumentskyddsförordningen). I artikel 9.4 g) ges den behöriga myndigheten befogenhet att beordra en värdtjänstleverantör att ta bort eller förhindra eller begränsa åtkomst till ett onlinegränssnitt. Någon närmare definition av begreppet värdtjänstleverantör finns inte i den förordningen.

I Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG (upphovsrättsdirektivet), finns bestämmelser om skyldigheter för

[9] Prop. 2001/02:150 *Lag om elektronisk handel och andra informationssamhällets tjänster, m.m.*, s. 18–19, jfr skäl 17 och 18 e-handelsdirektivet.

onlineleverantörer av delningstjänster för innehåll.[10] Onlineleverantörer av delningstjänster för innehåll är ett begrepp som har vissa likheter med TCO-förordningens värdtjänstleverantör. I artikel 2.6 upphovsrättsdirektivet definieras begreppet som en leverantör av en av informationssamhällets tjänster som har som huvudsyfte eller ett av sina huvudsyften att lagra och ge allmänheten tillgång till en stor mängd upphovsrättsskyddade verk eller andra skyddade alster som laddats upp av dess användare, som leverantören ordnar och marknadsför i vinstsyfte. I artikel 17 följer vissa skyldigheter för onlineleverantörer av delningstjänster för innehåll som använder skyddat innehåll.

Slutligen kan även nämnas Europeiska kommissionens förslag till en ny förordning rörande den inre digitala marknaden inom EU; Europaparlamentets och rådets förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 2000/31/EG, Bryssel den 15 december 2020, COM(2020) 825 final.[11] I fortsättningen kallad Digital Services Act eller DSA. I artikel 2 (f) definieras förmedlingstjänster som en av följande tjänster:

– En tjänst som enbart avser vidarefordran (*mere conduit*) och som består av överföring i ett kommunikationsnät av information som tillhandahållits av en tjänstemottagare, eller tillhandahållande av tillgång till ett kommunikationsnät.
– En *cachningstjänst* som utgörs av överföring i ett kommunikationsnät av information som tillhandahållits av en tjänstemottagare, och som innefattar automatisk, mellanliggande och tillfällig lagring av informationen enbart för att effektivisera den vidare överföringen av informationen till andra tjänstemottagare på deras begäran.
– En *värdtjänst* som utgörs av lagring av information som tillhandahålls av tjänstemottagaren och som sker på dennes begäran.

[10] Eng. *an online content-sharing service provider.*
[11] Förslaget är föremål för trepartsförhandlingar mellan Europaparlamentet, rådet och Europeiska kommissionen varför lydelsen kan komma att ändras.

4.3.3 Undantag från förordningen – vidarebefordranstjänster och cachningstjänster

När information överförs över internet mellanlagras den automatiskt i delar eller i dess helhet på olika servrar och routrar. Leverantörer av sådana vidarebefordranstjänster (mere conduit) eller cachningstjänster samt andra tjänster som tillhandahålls på andra nivåer av internetinfrastrukturen omfattas inte av TCO-förordningens tillämpningsområde. Här avses till exempel register och registrarer samt leverantörer av domännamnssystem (DNS), betalningstjänster eller skyddstjänster mot samordnad överbelastningsattack (DdoS).

Interpersonella kommunikationstjänster så som e-post och privata meddelanden omfattas inte heller av TCO-förordningen (se skäl 14 jfr artikel 2.5 i Europaparlamentets och rådets direktiv (EU) 2018/1972).

Begreppen vidarebefordranstjänster och cachningstjänster finns sedan tidigare i e-handelsdirektivet vilket genomförts i Sverige genom e-handelslagen. Vidarebefordranstjänster förklaras i förarbetena till e-handelslagen som tillhandahållandet av ledningar eller motsvarande (till exempel kopparkabel, fiberoptisk kabel eller satellitöverföring) och de datorer hos internetleverantörer, webb- eller e-postservrar, serverprogram och routrar som är nödvändiga för vidarebefordran.[12]

Cachningstjänster (eller cachelagringstjänster) innebär att information tillfälligt mellanlagras för att effektivisera vidare överföring av informationen. Servercachning eller proxycachning innebär att en internetleverantör lagrar webbsidor på lokala mellanservrar som är de servrar som vidarebefordrar trafiken mellan det interna och det externa nätet. I samma proposition som nämnts ovan förklaras även att cachning är när webbsidor som har många besökare lagras på en server närmare användaren. De som besöker sidan behöver då inte samtidigt styras till den ursprungliga sidans server, utan kan i stället styras till de cachekopior som ligger närmst användaren. Kopiorna gör att belastningen på nätet minskar och att det går fortare att ladda ned information. Möjligheten till cachning innebär därför att användaren upplever internet som snabbare och effektivare.[13]

[12] Prop. 2001/02:150 s. 20.
[13] Prop. 2001/02:150 s. 21.

4.3.4 Utredningens bedömning

Utredningens bedömning: För att en värdtjänstleverantör och dess värdtjänst ska omfattas av TCO-förordningen ska följande rekvisit vara uppfyllda:

1. Det ska vara fråga om *lagring* av innehåll,
2. som sker på *begäran* av innehållsleverantören, och
3. innehållet ska *spridas till allmänheten*.

Utredningen bedömer att till exempel följande tjänster kan uppfylla rekvisiten ovan och därför omfattas av förordningen:

- Webbsidor, med undantag för de som skyddas av yttrandefrihetsgrundlagen och tryckfrihetsförordningen.
- Sociala medietjänster, video-, bild- och ljuddelningstjänster.
- Molntjänster.
- Webbhotell.
- Onlinespel.
- Sökmotorer/söktjänster.

Utredningen bör inte uttala sig om tillämpningen av TCO-förordningen eller förtydliga innebörden av begrepp som förekommer i förordningen. Förordningen äger omedelbar tillämpning i svensk rätt. Tolkningen av begreppen värdtjänstleverantör och värdtjänst är förbehållet de myndigheter och domstolar som kommer att tillämpa förordningen i respektive medlemsstat. I sista hand har EU-domstolen tolkningsrätt.

Huruvida en viss värdtjänstleverantör omfattas av TCO-förordningens tillämpningsområde kommer att avgöras i varje enskilt ärende, utifrån omständigheterna i det ärendet, av den behöriga myndigheten och, om ärendet överklagas, av domstol. Först när förordningen börjar tillämpas kommer det att växa fram närmare rättslig vägledning för hur begreppen ska förstås.

Under utredningens arbete har begreppen ”värdtjänstleverantör” och ”värdtjänst” återkommande varit föremål för diskussion, bland

annat i kontakt med företrädare för it- och telekombranschen. Det har framkommit en osäkerhet kring vilka aktörer som kommer att anses vara värdtjänstleverantör i förordningens mening och därför omfattas av skyldigheterna i förordningen. För att möjliggöra en effektiv tillämpning av TCO-förordningen problematiserar utredningen nedan rekvisiten i förordningen samt applicerar rekvisiten på några olika tjänster som kan komma att anses vara värdtjänster i förordningens mening. Uppräkningen ska inte uppfattas som uttömmande.

TCO-förordningen kopplar samman begreppet värdtjänstleverantör, genom hänvisningen till artikel 1b i Europaparlamentets och rådets direktiv (EU) 2015/1535, med aktörer som utför kommersiella aktiviteter (tjänster) av något slag. En utgångspunkt är därmed att det är kommersiella tjänster, och inte ideella aktiviteter, som omfattas av förordningen.

I TCO-förordningen framgår det tre kumulativa rekvisit i artikel 2 och skäl 13–14 som ska vara uppfyllda för att det ska vara fråga om en värdtjänstleverantör som omfattas av förordningen:

1. Det ska vara fråga om lagring av innehåll,

1. som sker på begäran av innehållsleverantören, och

2. innehållet ska spridas till allmänheten.

De kumulativa rekvisiten kan resultera i att vissa tjänster hos en leverantör träffas av TCO-förordningen samtidigt som andra tjänster som leverantören erbjuder faller utanför tillämpningsområdet.

Den behöriga myndigheten kan endast rikta en avlägsnandeorder och andra beslut mot en värdtjänstleverantör som lagrar och sprider information på begäran av en innehållsleverantör. Beslut enligt TCO-förordningen kan inte riktas mot aktörer i andra delar av internets infrastruktur. Även om den faktiska lagringen har utlokaliserats till en annan aktör (till exempel en molntjänst) är det den värdtjänstleverantör som får den direkta begäran från innehållsleverantören som omfattas av skyldigheterna i TCO-förordningen.

En lagringstjänst skulle i exemplet ovan inte uppfylla kravet på direkt begäran från innehållsleverantören och skulle därför falla utanför förordningens tillämpningsområde. En *fildelnings- eller annan molntjänst* skulle dock kunna omfattas av TCO-förordningen om tjänsten används för att göra den lagrade informationen tillgänglig för allmänheten på begäran av innehållsleverantören. Vanligtvis är dock

inte information som en innehållsleverantör lagrar i en molntjänst tillgänglig för allmänheten.

En annan slags tjänst som skulle kunna omfattas av TCO-förordningen är *sökordstjänster*. Sökordsannonsering, eller sökordsoptimering, är en tjänst som tillhandahålls av till exempel Google Adwords. Tjänsten innebär att utvalda sökord rankas högt vid en sökning på en viss sökmotor. När EU-domstolen tolkat artikel 14 i e-handelsdirektivet ansåg domstolen att en sökmotors tillhandahållande av sökordsannonsering (s.k. key word advertising) omfattas av e-handelsdirektivets definition av värdtjänst.[14] Eftersom en söktjänst lagrar information på begäran av en innehållsleverantör skulle tjänsten kunna omfattas av TCO-förordningen i den mån den också innebär spridning av information till allmänheten. Vad gäller automatisk indexering av webbplatser, dvs. indexering som sker av alla webbplatser utan en särskild begäran från innehållsleverantören, är rättsläget i viss mån oklart. Avsaknaden av en direkt begäran från innehållsleverantören talar för att en sådan tjänst inte omfattas av TCO-förordningens definition av värdtjänst.

Webbsidor lagrar och sprider vanligtvis innehåll till allmänheten på begäran av en innehållsleverantör. Innehåll på webbsidor som omfattas av yttrandefrihetsgrundlagen eller tryckfrihetsförordningen faller emellertid utanför TCO-förordningens tillämpningsområde (se utredningens överväganden under avsnitt 5.6).

Andra tjänster som skulle kunna omfattas av TCO-förordningen är *webbhotell*. Webbhotell erbjuder uthyrning av lagringsutrymme. Om en användare vill göra en webbsida tillgänglig via internet, men inte har en egen webbserver med permanent internetuppkoppling, kan användaren hyra lagringsutrymme av ett webbhotell. Sådana tjänster tillhandahålls oftast av teleoperatörer, men även av andra tjänstetillhandahållare med s.k. portaler (webbsidor med ingångar till ett stort utbud av tjänster).

En annan form av tjänst som kan komma att omfattas av TCO-förordningen är så kallade *elektroniska anslagstavlor* (på engelska Bulletin Board System, BBS). En elektronisk anslagstavla är ett interaktivt sätt att möjliggöra kommunikation elektroniskt, till exempel genom inlägg i ett diskussionsforum eller kommentatorsfält på en webbsida. Elektroniska anslagstavlor regleras i BBS-lagen (se vidare i avsnitt 10.2). Gemensamt för dessa tjänster är att en användare både

[14] Se mål C-236/08 – Google France och Google.

kan föra in text och annan information på den elektroniska anslagstavlan samt ta del av information som andra har fört in.

Även *onlinespel* kan innehålla en möjlighet för användare att tillföra innehåll som lagras i spelet och som kan spridas till andra användare i spelet. Onlinespel skulle därför också kunna utgöra en värdtjänst i TCO-förordningens mening.

Slutligen framgår det av skäl 14 att TCO-förordningen ska omfatta leverantörer av *sociala medietjänster*, *video-*, *bild- och ljuddelningstjänster*, i den mån dessa tjänster används för att göra den lagrade informationen tillgänglig för allmänheten på direkt begäran av innehållsleverantören.[15]

[15] Skyldigheter för leverantörer av videodelningsplattformar regleras sedan tidigare i 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 (direktivet om audiovisuella medietjänster), mot bakgrund av ändrade marknadsförhållanden. Enligt skäl 8 i TCO-förordningen ska AV-direktivet inte påverka skyldigheterna enligt TCO-förordningen vad gäller leverantörer av videodelningsplattformar. Se avsnitt 10.4.3 för utredningens överväganden och förslag till komplettering av svensk rätt med anledning därav.

5 TCO-förordningens förhållande till yttrande- och informationsfrihet

5.1 Allmänna utgångspunkter

Formerna för publicering av innehåll på internet har utvecklats snabbt och är i ständig förändring. Vi har gått från att ta del av information ur tryckta skrifter och från radio och tv, till att i allt högre grad konsumera information som finns tillgänglig på internet. Internet innehåller dock inte enbart innehåll som är av godo. Olika aktörer använder internet som verktyg för att sprida olagligt innehåll, till exempel innehåll som på olika sätt bidrar till terrorism och terrorattentat.

TCO-förordningen innebär, särskilt ur yttrandefrihetssynpunkt, en helt ny form av rättsligt verktyg för att motverka spridning av terrorisminnehåll på internet. Möjligheten att med rättsligt bindande verkan besluta att en värdtjänstleverantör inom en timme ska avlägsna, eller göra oåtkomligt, visst innehåll på internet är en nyhet i svensk lagstiftning. Även andra delar av förordningen, till exempel att utöva tillsyn över värdtjänstleverantörer och att påföra dem sanktioner vid överträdelser, saknar motsvarighet sedan tidigare i svensk rätt.

Den befintliga lagen (1998:112) om ansvar för elektroniska anslagstavlor (BBS-lagen) har vissa beröringspunkter med TCO-förordningen, särskilt när det kommer till bestämmelsen i 5 § om en skyldighet att ta bort vissa meddelanden. Skyldigheten i BBS-lagen innebär att om en användare skickar in ett meddelande till en elektronisk anslagstavla ska tillhandahållaren av tjänsten ta bort meddelandet från tjänsten eller på annat sätt förhindra vidare spridning av meddelandet, om meddelandets innehåll uppenbart är sådant som avses i bestämmelserna om till exempel uppvigling i 16 kap. 5 § brottsbalken, hets mot folkgrupp i 16 kap. 8 § brottsbalken, olaga våldsskildring i 16 kap. 10 c § brottsbalken eller offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avse-

ende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen). I prop. 2021/22:133 *En samlad straffrättslig terrorismlagstiftning* föreslår regeringen vissa ändringar av bland annat 5 § BBS-lagen med anledning av den nya terroristbrottslag som samtidigt föreslås. Förslaget innebär att 5 § BBS-lagen i stället ska hänvisa till bestämmelsen om offentlig uppmaning i terroristbrottslagen.[1]

BBS-lagen omfattar således delvis annat innehåll än enbart det som TCO-förordningen definierar som terrorisminnehåll. Lagen är dock mer begränsad genom att den endast är tillämplig på elektroniska anslagstavlor (se mer under avsnitt 10.2). BBS-lagens förhållande till yttrande- och informationsfrihet är uttryckligen reglerat i 2 § tredje punkten. Där framgår att BBS-lagen inte gäller sådana tjänster som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Att motverka spridning av yttranden och annan information på internet tangerar frågor om grundläggande fri- och rättigheter, och yttrande- och informationsfrihet i synnerhet. I svensk rätt regleras rätten till yttrande- och informationsfrihet främst i regeringsformen, tryckfrihetsförordningen och yttrandefrihetsgrundlagen. De två senare benämns ibland yttrandefrihetsgrundlagarna. Därutöver regleras rättigheterna även i Europeiska konventionen om skydd för de mänskliga rättigheterna och grundläggande friheterna (Europakonventionen eller EKMR) och Europeiska unionens stadga om de grundläggande rättigheterna (EU:s stadga).

Det framgår uttryckligen av kommittédirektiven att utredningen vid sina överväganden noga ska beakta skyddet för grundläggande fri- och rättigheter, däribland yttrande- och informationsfriheten. En viktig fråga för utredningen är därför att analysera TCO-förordningens förhållande till de nationella yttrandefrihetsgrundlagarna. Det ingår dock inte i utredningens uppdrag att föreslå grundlagsändringar.

I TCO-förordningen regleras förhållandet till grundläggande fri- och rättigheter i artikel 1.4. Där framgår att TCO-förordningen inte ska innebära 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 grundläggande principer som rör yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald.

I detta kapitel redogör utredningen för rätten till yttrande- och informationsfrihet ur ett internetperspektiv och drar slutsatser kring

[1] Prop. 2021/22:133 s. 23 f.

när innehåll som publiceras på internet kan omfattas av grundlagsskydd. Kapitlet avser också att ge svar på följande frågor: Vad innebär det för TCO-förordningens tillämpning att innehåll är skyddat av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen? Vad innebär det om innehåll faller utanför yttrandefrihetsgrundlagarnas tillämpningsområde men alltjämt omfattas av den allmänna regleringen i regeringsformen?

5.2 Europakonventionen och EU:s stadga

Rätten till yttrandefrihet regleras i artikel 10.1 i EKMR.

> Var och en har 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. Denna artikel hindrar inte en stat att kräva tillstånd för radio-, televisions- eller biografföretag.

Europadomstolen har i ett rättsfall från 1976 uttryckt att yttrandefriheten utgör en av de väsentliga grundvalarna i ett demokratiskt samhälle, den omfattar inte endast information och idéer som mottas positivt eller anses ofarliga utan också de som kränker, chockerar eller stör staten eller någon del av befolkningen. Domstolen uttalade vidare att detta är de krav som ställs av den pluralism, den tolerans och den vidsynthet utan vilka inget ”demokratiskt samhälle” kan existera.[2]

Om vissa särskilda förutsättningar är för handen kan rätten till yttrandefrihet begränsas (artikel 10.2). En begränsning måste vara nödvändig i ett demokratiskt samhälle till exempel med hänsyn till den nationella säkerheten, den territoriella integriteten, den allmänna säkerheten, till förebyggande av oordning eller brott eller till skydd för hälsa eller moral. Åtgärder som begränsar rätten till yttrandefrihet ska vara proportionerliga. 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.

I EU:s stadga skyddas rätten till yttrandefrihet i artikel 11 där det framgår att var och en har rätt till yttrandefrihet som innefattar åsiktsfrihet samt frihet att ta emot och sprida uppgifter och tankar utan offentlig myndighets inblandning och oberoende av territoriella gränser, liksom att mediernas frihet och mångfald ska respekteras.

[2] Europadomstolens dom den 7 december 1976 i målet Handyside mot Förenade kungariket.

Rättigheternas räckvidd och möjlighet till begränsning regleras i artikel 52.1 EU:s stadga där det anges att varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan ska framgå av lag och vara förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av EU eller behovet av skydd för andra människors rättigheter och friheter.

5.3 Regeringsformen

I regeringsformen tillförsäkras var och en, gentemot det allmänna, vissa grundläggande fri- och rättigheter, däribland 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 § och 2 kap. 1 § regeringsformen). Av den senare bestämmelsen 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 § regeringsformen). Tryckfrihetsförordningen och yttrandefrihetsgrundlagen gäller vissa framställningsformer och är oberoende av innehållet i mediet, dvs. grundlagarna är innehållsneutrala.

Hänvisningen till tryckfrihetsförordningen och yttrandefrihetsgrundlagen i regeringsformen innebär att lagarna är lex specialis (speciallag) i förhållande till regeringsformen. Bestämmelserna om yttrande- och informationsfrihet i regeringsformen är därför tillämpliga när det inte är fråga om ett media som faller inom tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde.

När regeringsformen är tillämplig tillämpas de ordinarie straff- och processrättsliga lagarna i stället för den särskilda rättegångsordning

och brottskatalog som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Yttrande- och informationsfriheten i regeringsformen är inte absolut, utan kan begränsas under vissa förutsättningar. En begränsning kan endast ske genom lag för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Den får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett begränsningen och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. En begränsning får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 § regeringsformen).

Därutöver får yttrande- och informationsfriheten endast begränsas med hänsyn till rikets säkerhet, folkförsörjningen, allmän ordning och säkerhet, enskildas anseende, privatlivets helgd eller förebyggandet och beivrandet av brott. I övrigt får begränsningar av yttrande- och informationsfriheten endast göras om särskilt viktiga skäl föranleder det. När lagstiftaren överväger en begränsning ska särskilt beaktas vikten av vidaste möjliga yttrande- och informationsfrihet i politiska, religiösa, fackliga, vetenskapliga och kulturella angelägenheter (2 kap. 23 § regeringsformen).

5.4 Tryckfrihetsförordningen

Tryckfriheten syftar till att säkerställa ett fritt meningsutbyte, en fri och allsidig upplysning och ett fritt konstnärligt skapande. Tryckfriheten innebär vidare en frihet för var och en att i tryckt skrift uttrycka tankar, åsikter och känslor samt att offentliggöra allmänna handlingar och i övrigt lämna uppgifter i vilket ämne som helst. Var och en har rätt att ge ut skrifter utan att en myndighet eller ett annat allmänt organ hindrar detta i förväg. Ingen får straffas för en skrifts innehåll i andra fall än om innehållet strider mot tydlig lag som är meddelad för att bevara allmänt lugn men som inte håller tillbaka allmän upplysning (1 kap. 1 § tryckfrihetsförordningen).

Tryckfrihetsförordningen är en speciallag i förhållande till yttrande- och informationsfriheten i regeringsformen. Grundlagen gäller för skrifter som framställs i tryckpress och, om samtliga förutsättningar är uppfyllda, för skrifter som har mångfaldigats genom fotokopiering eller liknande teknik (1 kap. 2 § tryckfrihetsförordningen).

Tryckfrihetsförordningen kan i vissa fall bli tillämplig på innehåll som publiceras på internet om det är fråga om innehåll i en tryckt periodisk skrift som är skyddad enligt tryckfrihetsförordningen och i oförändrat skick även publiceras på internet. En sådan publicering kan under vissa förutsättningar omfattas av grundlagsskyddet i tryckfrihetsförordningen enligt de s.k. bilagereglerna (1 kap. 5–6 §§). I praktiken kan det ske till exempel om en tryckt bok även publiceras som e-bok. E-boken kan då komma att omfattas av grundlagsskyddet om förutsättningarna i 1 kap. 6 § är uppfyllda. Den som ansvarar för skriften blir då även ansvarig för innehållet när det publiceras på internet.

Utrymmet för att innehåll som publiceras på internet omfattas av grundlagsskyddet i tryckfrihetsförordningen är i praktiken mycket begränsat. I det fall material på internet omfattas av grundlagsskydd är det framför allt genom bestämmelser i yttrandefrihetsgrundlagen, se nedan.

5.5 Yttrandefrihetsgrundlagen

Yttrandefrihetsgrundlagens syfte är att garantera var och en, mot det allmänna, en rätt att i vissa framställningsformer offentligt uttrycka sina tankar, åsikter och känslor och i övrigt lämna uppgifter i vilket ämne som helst (1 kap. 1 § yttrandefrihetsgrundlagen).

Yttrandefrihetsgrundlagen har utformats med tryckfrihetsförordningen som förebild och innehåller flera principer som även kommer till uttryck i tryckfrihetsförordningen, till exempel principen om etableringsfrihet, ensamansvar, förbud mot censur och exklusivitetsprincipen.

Förbudet mot censur och andra hindrande åtgärder innebär ett skydd mot förhandsgranskning av det allmänna i syfte att godkänna eller förbjuda publicering. Det är också ett skydd mot andra sätt att hindra framställning, utgivning och spridning av material som skyddas av yttrandefrihetsgrundlagen (1 kap. 11 §). Skyddet gäller i förhållande till det allmänna och innebär inget hinder mot att juridiska personer, till exempel värdtjänstleverantörer, ingår avtal med användare om att innehåll som publiceras på värdtjänsten filtreras eller på annat sätt granskas och censureras.[3]

[3] Axberger, Hans-Gunnar, *Yttrandefrihetsgrundlagarna* (2019, version 4, JUNO) s. 88.

Justitiekanslern har uttalat sig om censurförbudets betydelse och innebörd i ett beslut som meddelades den 24 mars 2006 (dnr JK 1319-06-21). Ärendet handlade om huruvida Säkerhetspolisen och en företrädare för Utrikesdepartementet agerat i strid med censurförbudet genom att ta vissa kontakter med företrädare för ett webbhotell och en grundlagsskyddad webbsida. Justitiekanslern uttalade följande i beslutet:

> Censurförbudet är en av de hörnpelare på vilka den svenska tryck- och yttrandefriheten vilar. Att en fri och obunden debatt kan äga rum utan några i förväg lagda hinder från statsmakternas sida är en omistlig del i vårt demokratiska statsskick, liksom att kritik fritt kan framföras och information flöda utan hinder. Censurförbudet utgör ytterst en garanti för detta.
>
> Censurförbudet innebär bl.a. att det är förbjudet för myndigheter och andra allmänna organ att utan stöd i yttrandefrihetsgrundlagen på grund av det kända eller väntade innehållet på t.ex. en grundlagsskyddad hemsida förbjuda eller hindra dess offentliggörande eller spridning bland allmänheten. Att företrädare för det offentliga fysiskt eller genom hot ser till att en hemsida stängs strider sålunda mot detta förbud. Även vissa påtryckningar som leder till stängning kan innebära ett brott mot förbudet.

Justitiekanslern fann i beslutet att det saknades anledning att rikta kritik mot Säkerhetspolisens agerande. Det framkom också i ärendet att företrädare för Utrikesdepartementet hade tagit kontakterna först efter samråd med statsrådet som var den Justitiekanslern ansåg hade ansvaret för kontakten. Eftersom statsråd inte står under Justitiekanslerns tillsyn utan granskas av Riksdagens konstitutionsutskott, uttalade sig Justitiekanslern inte närmare om statsrådets agerande.

Exklusivitetsprincipen i 1 kap. 14 § yttrandefrihetsgrundlagen innebär att om ett yttrande eller innehåll omfattas av yttrandefrihetsgrundlagen är endast yttrandefrihetsgrundlagens regler tillämpliga. Inga andra åtgärder eller sanktioner än de som framgår av yttrandefrihetsgrundlagen kan vidtas mot sådant innehåll. Utredningen återkommer nedan till principens betydelse för TCO-förordningens tillämpning.

Som framgått ovan är yttrandefrihetsgrundlagen tillämplig på vissa särskilda framställningsformer. Tillämpningsområdet kan delas in i två kategorier där den första omfattar överföringar av ljud, bild eller text som sker med elektromagnetiska vågor och den andra kategorin omfattar tekniska upptagningar (1 kap. 1 §). Den förra kategorien avser, annorlunda uttryckt, traditionella radio- och tv-sändningar, webb-

sändningar samt viss annan publicering på internet. Den senare kategorin omfattar fysiska informationsbärare till exempel filmer och upptagningar på band.

Vid överföringar med elektromagnetiska vågor utgår yttrandefrihetsgrundlagen från begreppet *program*. En sändning av ett program ska vara riktad till allmänheten och avsedd att tas emot med ett tekniskt hjälpmedel (1 kap. 3 § första stycket). Det som avses här är främst linjära (traditionella) radio- och tv-program. Även direktsända eller inspelade program som tillhandahålls allmänheten på särskild begäran på internet jämställs i lagen med program (s.k. webbsändningar) under förutsättning att programmets starttidpunkt och innehåll inte kan påverkas av mottagaren.

Bestämmelserna om sändningar av program tillämpas även när vissa aktörer tillhandahåller allmänheten information ur en databas, vars innehåll kan ändras endast av den som driver verksamheten, med hjälp av elektromagnetiska vågor. Innehåll som publiceras på internet kan omfattas av denna regel (1 kap. 4 §, även kallad databasregeln, se vidare nedan).

5.5.1 I vilken omfattning kan innehåll på internet omfattas av YGL?

Utgångspunkten är att innehåll som publiceras på internet inte omfattas av yttrandefrihetsgrundlagen. Det finns dock vissa undantag. För att analysera TCO-förordningens förhållande till yttrandefrihetsgrundlagen redogör utredningen nedan för vilket innehåll på internet som kan omfattas av grundlagens tillämpningsområde.

Särskilt om databasregeln

Databasregeln i 1 kap. 4 § yttrandefrihetsgrundlagen innebär att bestämmelserna om sändningar av program också tillämpas när information ur en databas, vars innehåll kan ändras endast av den som driver verksamheten, tillhandahålls allmänheten med hjälp av elektromagnetiska vågor

1. av någon av följande:

   a) en redaktion för en periodisk skrift eller ett program,

b) ett företag för yrkesmässig framställning av sådana skrifter som avses i tryckfrihetsförordningen eller av tekniska upptagningar,

c) en nyhetsbyrå, eller

d) någon annan, om det finns utgivningsbevis för verksamheten enligt 5 §, och

2 på något av följande sätt:

a) överföring på särskild begäran,

b) överföring enligt överenskommelse i förväg,

c) framställning av tekniska upptagningar, skrifter eller bilder, eller

d) offentlig uppspelning.

De sätt som avses under punkten 2 innebär i praktiken följande. Överföring på särskild begäran a) är enklare uttryckt traditionell databasverksamhet, till exempel tillhandahållande av information från webbsidor på särskild begäran eller play-tjänster så som SVT Play eller Netflix. Vid överföring på särskild begäran är det, till skillnad från webbsändningsregeln, mottagaren som väljer att starta sändningen, till exempel ett program på en play-tjänst. Det avgörande är att innehållet endast kan ändras av avsändaren och inte av mottagaren. Materialet ska vara riktat mot allmänheten dvs. tillgängligt för alla och inte publiceras i ett slutet nät så som till exempel en arbetsgivares intranät. Kravet på tillgänglighet hindrar inte att det krävs medlemskap eller att användare måste betala för att ta del av materialet.

Överföring enligt överenskommelse i förväg b) är det som ofta benämns push-notiser, till exempel utskick av elektroniska nyhetsbrev från ett företag till dess prenumeranter.

Framställning av tekniska upptagningar, skrifter eller bilder c) kallas även print-on-demand och innebär att det ur en databas på särskild begäran beställs fysiska exemplar av materialet. Här kan nämnas att regeringen föreslår i propositionen *Ett ändamålsenligt skydd för tryck- och yttrandefriheten* att ”på särskild begäran” läggs till i punkten c).

Förslaget är inte tänkt att förändra rättsläget utan är snarare av rättelsekaraktär.[4]

Slutligen är offentlig uppspelning d) vanligtvis digital bio där filmen spelas upp från en databas och inte från en teknisk upptagning, till exempel vid utomhusbio. Offentlig uppspelning kan också vara när publik tar del av teater, konsert eller sportevenemang från en digital källa.[5]

De aktörer som räknas upp i 4 § första punkten a)–c) får genom databasregeln ett automatiskt grundlagsskydd för material som de publicerar på internet. Det är de traditionella massmedieföretagen; redaktioner för tryckta periodiska skrifter eller för program, företag för yrkesmässig framställning av tekniska upptagningar och nyhetsbyråer. Databaser med automatiskt grundlagsskydd ska anmälas till Myndigheten för press, radio och tv. Drygt 1 500 databaser med automatiskt grundlagsskydd finns i dagsläget registrerade hos myndigheten.[6]

Om en viss del av ett massmedieföretags webbsida innehåller material som tillförs av någon annan gäller skyddet i yttrandefrihetsgrundlagen endast för de delar av webbsidan som innehåller material som publicerats av massmedieföretaget.[7]

En annan kategori av aktörer som omfattas av databasregeln är de aktörer som sökt och beviljats s.k. utgivningsbevis och på så sätt erhållit ett frivilligt grundlagsskydd för sin databas. Utgivningsbevis söks normalt av företag eller privatpersoner som enbart publicerar material på internet så som till exempel på en blogg, en nyhetswebbsida eller i en app. Ansökan om utgivningsbevis görs till Myndigheten för press, radio och tv. För att erhålla utgivningsbevis är ett krav att det finns en ansvarig utgivare för databasen. Den ansvarige utgivaren måste vara myndig, inte försatt i konkurs eller stå under förmyndare och vara folkbokförd i Sverige. Myndigheten för press, radio och tv gör ingen prövning av vilket innehåll som är tänkt att tillhandahållas. Prövningen består endast av en kontroll av om de formella förutsättningarna är uppfyllda för att utfärda ett utgivningsbevis (se 1 kap. 5 § yttrandefrihetsgrundlagen och lag [1991:1559] med föreskrifter på tryckfrihetsförordningens och yttrandefrihetsgrundlagens områden [tillämpningslagen]). För närvarande finns det nästan 1 600 regi-

[4] Prop. 2021/22:59 *Ett ändamålsenligt skydd för tryck- och yttrandefriheten*, s. 8 och 68.
[5] Axberger, Yttrandefrihetsgrundlagen (1991:1469) 1 kap. 4 §, Karnov 2021-11-10 (JUNO).
[6] www.mprt.se/tillstandsregister/ (hämtad 2022-03-16).
[7] Se 1 kap. 4 § andra stycket YGL och NJA 2014 s. 128.

strerade utgivningsbevis i Myndigheten för press, radio och tv:s tillståndsregister.

Myndigheten saknar möjlighet att återkalla ett utgivningsbevis med hänvisning till någon annan omständighet än bristande formella förutsättningar. Bestämmelsernas utformning innebär att aktörer som omfattas av det frivilliga grundlagsskyddet har databaser som tillhandahåller innehåll av vitt skilda slag, till exempel JP Infonet AB, Synskadades riksförbud och Mora kommun.[8]

Betydelsen av det frivilliga grundlagsskyddet belystes av Högsta domstolen i rättsfallet NJA 2021 s. 498. Målet rörde en film som publicerats på en webbsida med utgivningsbevis. Åtalet prövades därför enligt den särskilda rättegångsordningen och brottskatalogen i yttrandefrihetsgrundlagen. Frågan i målet var om den ansvarige utgivaren kunde dömas för yttrandefrihetsbrottet olaga våldsskildring för en publicering av gärningsmannens film från terrorattentatet i Christchurch, Nya Zeeland (2019). Filmen hade publicerats som en del av en artikel i anslutning till attentatet. Domstolen bedömde att filmen innehöll våldsskildringar som utgjorde olaga våldsskildring. Frågan var om publiceringen av filmen kunde anses försvarlig. Vid försvarlighetsbedömningen vägde domstolen allmänintresset av att visa våldsskildringen mot intresset bakom kriminaliseringen av olaga våldsskildring; att skydda främst barn och ungdomar mot de skadeverkningar som kan uppstå om de utsätts för grova våldsskildringar. Högsta domstolen kom fram till att publiceringen var försvarlig bland annat eftersom den skett i samband med nyhetsförmedling och att intresset för den rapporterade händelsen var stark vid tidpunkten. Åtalet för yttrandefrihetsbrott och olaga våldsskildring ogillades.

Särskilt om webbsändningsregeln

Direktsända och förinspelade program på internet som startas utan att mottagaren bestämmer starttidpunkten omfattas av webbsändningsregeln (1 kap. 3 § andra stycket yttrandefrihetsgrundlagen). Bestämmelsen skiljer sig från databasregeln framför allt genom att det här är avsändaren och inte mottagaren som bestämmer starttidpunkten för programmet. Skyddet är automatiskt och inte begränsat till vissa aktörer. Webbsändningar ska registreras hos Myndigheten

[8] Se Myndigheten för press, radio och tv:s hemsida www.mrpt.se (hämtad 2021-09-14).

för press, radio och tv. För närvarande har drygt 1 350 aktörer anmält webbsändningar hos myndigheten.[9]

Webbsändningsregeln har efter införandet ändrats flera gånger, bland annat har regeln förtydligats genom ett tillägg i databasregeln om att sändningar som omfattas av webbsändningsregeln är undantagna från databasregelns tillämpningsområde.[10]

Den tekniska utvecklingen har medfört att det numera förekommer webbsändningar i stor omfattning. Webbsändningsregeln har därför kommit att få ett bredare tillämpningsområde än bestämmelsens ursprungliga syfte. Frågan om grundlagsskyddets omfattning för webbsändningar har varit (och är) föremål för lagstiftningsåtgärder och prövning i Högsta domstolen.

I rättsfallet NJA 2018 s. 562 (Facebookmålet) prövade Högsta domstolen om ett övergrepp som direktsänts på Facebook kunde omfattas av webbsändningsregeln. Direktsändningen hade skett på en Facebooksida med cirka 60 000 medlemmar. Den åtalade beskrivs i domen som en relativt frekvent sändare på sidan. Domstolen uttalade att webbsändningsregeln kan omfatta sändningar av privatpersoner under förutsättning att materialet som sänds är ett *program* i yttrandefrihetsgrundlagens mening. Högsta domstolen kom fram till att ett övergrepp som direktsänds på Facebook inte omfattas av webbsändningsregeln eftersom begreppet program ska ges en viss självständig betydelse. Begreppet, menade domstolen, syftar på ett tematiskt avgränsat ljud- och bildinnehåll som normalt har ett namn och ingår i ett programutbud. Mot den bakgrunden menade domstolen att en sändning som i allt väsentligt är obestämd till format, inriktning och tid är inte ett program i webbsändningsregelns mening. Direktsändningen på Facebook omfattades därför inte av yttrandefrihetsgrundlagens regler.

Rättsfallet innebär att en sändning som i allt väsentligt är obestämd till format, inriktning och tid inte är ett program i webbsändningsregelns mening. Rättsfallet utesluter endast de mest spontana sändningar som sker utan någon som helst planering eller förberedelse från webbsändningsregelns tillämpningsområde.[11]

Utvecklingen av nya former av webbsändningar och dessas förhållande till yttrandefrihetsgrundlagen var en anledning till att 2018 års

[9] www.mprt.se/tillstandsregister/ (hämtad 2021-10-26).
[10] 1 kap. 4 § sista stycket YGL och prop. 2009/10:81 s. 47–49.
[11] Prop. 2021/22:59 s. 32.

tryck- och yttrandefrihetskommitté fick i uppdrag att överväga om grundlagsskyddet för webbsändningar var ändamålsenligt och väl avvägt. I betänkandet *Ett ändamålsenligt skydd för tryck- och yttrandefriheten* (SOU 2020:45) instämde utredningen i tidigare bedömningar; att databasregelns hänvisning till webbsändningsregeln kan tolkas som att andra webbsidor som en webbsändare driver också kan omfattas av grundlagsskyddet, även om den andra webbplatsen saknar anknytning till webbsändningen, så länge det anses vara samma redaktion som tillhandahåller webbsidorna.[12] Utredningen uttalade vidare att:

> Det finns skäl att utgå från att webbsändningar i yttrandefrihetsgrundlagens mening förekommer i mycket stor omfattning och att det är fråga om sändningar av vitt skilda slag.
>
> Genom den tekniska utvecklingen har webbsändningsregelns tillämpningsområde fått en sådan stor omfattning att regeln inte längre kan anses vara ändamålsenlig och väl avvägd. Även det förhållandet att den som tillhandahåller webbsändningar utgör en redaktion för ett program och därigenom har automatiskt grundlagsskydd för sina databaser talar för att webbsändningsregeln inte längre kan anses väl avvägd.[13]

Utredningen föreslog att webbsändningsregeln bör begränsas till att omfatta de webbsändningar som tillhandahålls av aktörer som omfattas av databasregeln, dvs. traditionella massmedieföretag och aktörer med utgivningsbevis. Vidare föreslog utredningen att redaktioner för webbsändningar bör undantas från databasregelns tillämpningsområde, vilket skulle få till följd att dessa inte längre har grundlagsskydd för sina databaser endast på den grunden att de webbsänder.[14]

Regeringen har i propositionen 2021/22:59 *Ett ändamålsenligt skydd för tryck- och yttrandefrihet* föreslagit att för att tillhandahållanden till allmänheten på särskild begäran av direktsända eller inspelade program ska anses som sändningar av program ska det krävas, utöver att starttidpunkten och innehållet inte kan påverkas av mottagaren, att programmen tillhandahålls av någon som omfattas av databasregeln. Därutöver föreslår regeringen att redaktioner som tillhandahåller enbart sådana program som avses i webbsändningsregeln undantas från det automatiska grundlagsskyddet enligt databasregeln. Hänvisningen från databasregeln till webbsändningsregeln ska därmed tas bort. Ändringarna föreslås träda i kraft den 1 januari 2023.[15]

[12] SOU 2020:45 s. 224.
[13] SOU 2020:45 s. 220.
[14] SOU 2020:45 s. 225.
[15] Prop. 2021/22:59 s. 33 f och 37 f.

Något kort om interaktiva medier

Innehåll som publiceras i interaktiva medier (sociala medier), så som Facebook eller Youtube, omfattas normalt inte av grundlagsskyddet i yttrandefrihetsgrundlagen bland annat eftersom verksamhetsutövaren saknar möjlighet att kontrollera material som en användare publicerar.[16]

Sociala mediers förhållande till yttrandefrihetsgrundlagen har varit föremål för diskussion i takt med att de traditionella massmedieföretagen i allt större omfattning kommit att använda och publicera innehåll i dessa medier. En fråga som i detta sammanhang diskuterats är om ett massmedieföretags publicering på en egen Facebooksida kan omfattas av databasregeln. I rättspraxis har sedan tidigare en viss del av en webbsida ansetts utgöra en egen enhet, om den är avskild från övrigt material.[17] Det synsättet talar för att ett massmedieföretags sida på till exempel Facebook kan utgöra en egen databas – skild från Facebook i övrigt – och i så fall omfattas av databasregeln. Mediegrundlagskommitténs bedömning av rättsläget i betänkandet *Ändrade mediegrundlagar* var att det inte är uteslutet att ett massmedieföretags avskilda ytor på sociala medier kan omfattas av det automatiska grundlagsskyddet enligt databasregeln.[18]

En annan omständighet som kan få betydelse för bedömningen är att värdtjänstleverantörer i dess användarvillkor ofta har en avtalad rätt att ta bort innehåll från sin tjänst. Facebook kan till exempel med stöd av sina användarvillkor ta bort visst innehåll som en användare publicerar på Facebook. Detta kan tala mot att en Facebooksida omfattas av databasregeln eftersom det då inte enbart är massmedieföretaget som råder över och kan ändra innehåll som publiceras på sidan.

Yttrandefrihetsgrundlagens territoriella tillämpning

För att besvara frågan vilket innehåll på internet som omfattas av yttrandefrihetsgrundlagen redogör utredningen nedan för yttrandefrihetsgrundlagens territoriella räckvidd.

---

[16] SOU 2020:45 s. 207–208 och Axberger, Hans-Gunnar, *Yttrandefrihetsgrundlagarna* (2019, version 4, JUNO) s. 58 och NJA 2014 s. 128 och 1 kap. 4 § andra stycket yttrandefrihetsgrundlagen.
[17] NJA 2014 s. 128.
[18] SOU 2016:58 *Ändrade mediegrundlagar*, s. 337 och Lagrådsremissen *Ett ändamålsenligt skydd för tryck- och yttrandefriheten*, s. 34–35.

Utgångspunkten är att yttrandefrihetsgrundlagen är tillämplig på tekniska upptagningar som framställs och sprids i Sverige samt på program och databasöverföringar som utgår från Sverige.[19] I 11 kapitlet yttrandefrihetsgrundlagen finns dock bestämmelser om som ger visst skydd för program och tekniska upptagningar från utlandet.

Yttrandefrihetsgrundlagen gäller både i förhållande till svenska medborgare och juridiska personer och i förhållande till utländska medborgare och juridiska personer. Såvitt avser utländska medborgare och juridiska personer kan yttrandefrihetsgrundlagens tillämpningsområde begränsas genom lag (12 kap. 3 § yttrandefrihetsgrundlagen).

Högsta domstolen har i rättsfallet NJA 2001 s. 445 prövat vilken anknytning till Sverige som bör krävas för att databasregeln ska vara tillämplig. Målet handlade, här i korthet, om en redaktion för en tryckt skrift som förmedlade viss information genom sändning från en server som fanns utanför Sverige. Den ansvarige åtalades för hets mot folkgrupp med anledning av ett föredrag som publicerats på en webbsida. Databasregeln i 1 kap. 4 § yttrandefrihetsgrundlagen innehåller inget uttryckligt krav på att innehållet på en webbsida ska göras tillgängligt från Sverige för att bestämmelsen ska vara tillämplig. Domstolen uttalade dock att det framstår som tydligt att viss anknytning till Sverige måste föreligga för att yttrandefrihetsgrundlagens ansvarssystem, som bland annat förutsätter att en utgivare kan utses enligt bestämmelserna i 4 kapitlet, ska vara tillämpligt på sådana sändningar som avses i databasregeln. Domstolen uttalade vidare att när det gäller informationsöverföring från en redaktion för en tryckt periodisk skrift innebär redan det förhållandet att skriften omfattas av tryckfrihetsförordningens regler om periodiska skrifter en tillräcklig anknytning. Detsamma måste gälla när information tillhandahålls av redaktionen för ett radioprogram som sänds från Sverige. I övriga fall får i avsaknad av närmare reglering ledning sökas i allmänna principer för räckvidden av offentligrättslig lagstiftning. Det kan då ha betydelse om företaget är verksamt i Sverige och om materialet är avsett för en svensk publik. I rättsfallet kom domstolen fram till att yttrandefrihetsgrundlagens ansvarighetsbestämmelser var tillämpliga på den aktuella informationsöverföringen.

[19] SOU 2020:45 s. 74 och 132.

5.6 Utredningens överväganden och förslag

Utredningens bedömning: TCO-förordningen och kompletteringslagen ska inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Bestämmelserna i TCO-förordningen utgör en godtagbar begränsning av yttrande- och informationsfriheten i regeringsformen.

Om en behörig myndighet i en annan medlemsstat handlägger ett ärende som rör innehåll hos en värdstjänstleverantör som har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare bosatt eller etablerad i Sverige kan den behöriga myndigheten i Sverige bistå den handläggande myndigheten med information om huruvida innehållet är skyddat av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, företrädesvis genom samverkan inom ramen för Europols kommande it-system, PERCI.

Om en annan medlemsstat utfärdar en order mot innehåll som skyddas av yttrandefrihetsgrundlagarna kan den behöriga myndigheten i Sverige inleda ett granskningsförfarande enligt artikel 4 i TCO-förordningen.

I detta avsnitt sammanfattar utredningen vilket innehåll på internet som kan omfattas av grundlagsskyddet i regeringsformen, tryckfrihetsförordningen eller yttrandefrihetsgrundlagen samt vilken betydelse det får för genomförandet och tillämpningen av TCO-förordningen i Sverige.

5.6.1 Skyddet för yttrande- och informationsfrihet i TCO-förordningen

TCO-förordningen har företräde framför svensk rätt så länge förordningen inte anger annat. Utgångspunkten är att det även gäller när det kommer till respektive medlemsstats grundlagar men frågan har varit, och är alltjämt, föremål för diskussion.[20]

Artikel 1.4 i TCO-förordningen uttrycker 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

[20] Se EU-domstolens avgöranden i målen Costa/ENEL (C-6/64) och Internationale Handelsgesellschaft (C-11/70) samt redogörelsen i SOU 2020:45 s. 100–103.

ska tillämpas utan att det påverkar tillämpningen av grundläggande principer som rör yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald. Artikel 6 i EU-fördraget innehåller i sin tur en hänvisning till de rättigheter, friheter och principer som kommer till uttryck i EU:s stadga samt en upplysning om att de grundläggande rättigheterna, som garanteras i EKMR, och som följer av medlemsstaternas gemensamma konstitutionella traditioner, ska ingå i unionsrätten som allmänna principer.

Syftet med TCO-förordningen är att bidra till att skydda den allmänna säkerheten, samtidigt som lämpliga och stabila skyddsåtgärder fastställs för att säkerställa skyddet för grundläggande rättigheter, vilket bland annat inbegriper rätten till yttrandefrihet, rätten att ta emot och sprida information och rätten till ett effektivt rättsmedel. Behöriga myndigheter och värdtjänstleverantörer ska endast vidta åtgärder som är nödvändiga, lämpliga och proportionerliga i ett demokratiskt samhälle, med beaktande av den särskilda vikt som tillmäts yttrande- och informationsfriheten (skäl 10).

Vid bedömningen av om visst innehåll på internet är terrorisminnehåll ska den behöriga myndigheten särskilt beakta rätten till yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald. Vidare lyfts det fram i skäl 12 att om en innehållsleverantör har ett redaktionellt ansvar bör varje beslut beakta de publicistiska normer som fastställs genom press- eller medieregleringen i enlighet med unionsrätten, inklusive EU:s stadga.

5.6.2 Syftet med publiceringen

Innehåll som sprids på internet i vissa godtagbara syften undantas från TCO-förordningens tillämpningsområde. Sådant innehåll kan inte bli föremål för de åtgärder som följer av TCO-förordningen. Det är här fråga om innehåll som sprids 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 (skäl 12).

Undantaget betyder att innehåll på internet, som i och för sig också kan omfattas av grundlagsskyddet i yttrandefrihetsgrundlagen, faller utanför förordningens tillämpningsområde redan på den grund

att innehållet publicerats med ett godtagbart syfte. I praktiken kan det vara journalistiska artiklar som förmedlar nyheter eller innehåll som sprids i utbildningssyfte. Även debattartiklar där individer uttrycker radikala, polemiska eller kontroversiella åsikter i den offentliga debatten om känsliga politiska frågor ska kunna spridas på internet utan att det anses vara terrorisminnehåll.

Om den behöriga myndigheten bedömer att en publicering skett med något av de uppräknade syftena är TCO-förordningen inte tillämplig på innehållet och den behöriga myndigheten saknar anledning att göra någon ytterligare bedömning.

5.6.3 Betydelsen av skyddet för yttrande- och informationsfrihet i yttrandefrihetsgrundlagen

Om innehållet inte omfattas av något av de godtagbara syftena i TCO-förordningen aktualiseras frågan om innehållet är skyddat av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen och betydelsen av ett sådant skydd.

Rätten till yttrande- och informationsfrihet tillmäts historiskt sett stor vikt i svensk rätt. Yttrandefrihetsgrundlagarna som skyddar yttrande- och informationsfriheten bygger på exklusivitetsprincipen. Principen är ovanlig i ett europeiskt perspektiv och innebär att innehåll som sprids till allmänheten i ett grundlagsskyddat media enbart ska bli föremål för de åtgärder och sanktioner som följer av tryckfrihetsförordningen respektive yttrandefrihetsgrundlagen. Dessa exklusiva system omfattar bland annat principen om ensamansvar, en särskild brottskatalog och en särskild rättegångsordning.

När det kommer till innehåll som publiceras på internet är utgångspunkten att det inte omfattas av skyddet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Det finns dock flera undantag som innebär att innehåll som sprids på internet, under vissa förutsättningar, kan omfattas av grundlagsskydd, främst yttrandefrihetsgrundlagen (jfr vad utredningen konstaterat ovan om tryckfrihetsförordningens tillämpning på innehåll på internet).

För att yttrandefrihetsgrundlagen ska vara tillämplig ska innehållet inte kunna ändras eller påverkas av användaren eller mottagaren. Vidare ska den som är ensam ansvarig för innehållet, normalt den ansvarige utgivaren, ha en faktisk kontroll över innehållet. Det innebär att innehåll på interaktiva medier, till exempel sociala medier där det

är användaren som råder över vad som publiceras, som regel inte omfattas av yttrandefrihetsgrundlagen. Att vidta åtgärder mot innehåll som sprids på sociala medier strider därför normalt[21] inte mot yttrandefrihetsgrundlagen.

Yttrandefrihetsgrundlagen kan skydda innehåll på internet som omfattas av databasregeln och antingen publiceras av de traditionella massmedieföretagen eller av en aktör som sökt och beviljats utgivningsbevis (1 kap. 4 § yttrandefrihetsgrundlagen). Även en webbsändning som uppfyller förutsättningarna i 1 kap. 3 § yttrandefrihetsgrundlagen kan omfattas av grundlagsskyddet. Såvitt avser webbsändningsregeln kan här åter påpekas att det pågår ett lagstiftningsarbete som innebär, om det antas, att webbsändningsregeln kommer att begränsas eftersom skyddet för webbsändningar kommer att kopplas till de aktörer som omfattas av databasregeln. En sådan ändring innebär att en mängd innehåll som sprids på internet i framtiden kommer att falla utanför yttrandefrihetsgrundlagens tillämpningsområde.

Databasregelns och webbsändningsregelns tillämpningsområde leder utredningen till slutsatsen att en hel del material som publiceras på internet kan omfattas av yttrandefrihetsgrundlagen. Möjligheten att ansöka och relativt enkelt beviljas utgivningsbevis öppnar upp för att mängden material som omfattas av grundlagsskyddet är förändérlig och kan öka alternativt minska över tid. Utredningens bedömning är att innehåll som kan bli föremål för prövning enligt TCO-förordningen kan ha publicerats i ett grundlagsskyddat media.

Om den behöriga myndigheten bedömer att ett visst innehåll skyddas av yttrandefrihetsgrundlagen eller tryckfrihetsförordningen anser utredningen att rätten till yttrande- och informationsfrihet så som den kommer till uttryck i de svenska yttrandefrihetsgrundlagarna utgör ett uttryck för sådana grundläggande friheter som avses i artikel 1.4 TCO-förordningen. Skyddet och tillämpningen av grundlagarna ska därmed inte påverkas av TCO-förordningen. TCO-förordningen ska därför inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Den bedömningen är väl förenlig med det skydd för yttrande- och informationsfrihet och särskilt mediernas frihet och mångfald som kommer till uttryck i såväl artikel 1.4 TCO-förordningen som i flera av förordningens inledande skäl.

[21] Jfr dock diskussionen under avsnitt 5.5.1.

Innehåll som omfattas av yttrandefrihetsgrundlagarna, antingen genom ett automatiskt eller frivilligt grundlagsskydd, ska därför inte bli föremål för de åtgärder som följer av TCO-förordningen. Det innebär till exempel att innehåll som publiceras på en webbsida med utgivningsbevis inte kan träffas av en avlägsnandeorder eller andra åtgärder som beslutas med stöd av TCO-förordningen.

Innehåll som publiceras på en grundlagsskyddad webbsida kan i stället aktualisera ansvar för tryckfrihets- respektive yttrandefrihetsbrott enligt den särskilda brottskatalogen i tryckfrihetsförordningen och yttrandefrihetsgrundlagen och ett ensamansvar för den ansvarige utgivaren.[22] I det här sammanhanget kan särskilt nämnas yttrande- och tryckfrihetsbrotten *olaga hot*, *uppvigling*, *hets mot folkgrupp* och *olaga våldsskildring* (7 kap. tryckfrihetsförordningen och 5 kap. yttrandefrihetsgrundlagen). Av förarbetena till lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen) framgår det att offentlig uppmaning i 3 § den lagen motsvarar brottet uppvigling som finns såväl i brottsbalken som i tryckfrihetsförordningen och yttrandefrihetsgrundlagen.[23] Slutligen kan nämnas att det även finns skyldigheter i radio- och tv-lagen (2010:696) som kan träffa grundlagsskyddade medier.

5.6.4 Innehåll som omfattas av regeringsformen

Det kan även förekomma att innehåll som är föremål för prövning i ett TCO-ärende, och som inte omfattas av skyddet för yttrande- och informationsfrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen, i stället omfattas av den allmänna regleringen i regeringsformen.

De åtgärder som kan vidtas mot innehåll på internet med stöd av TCO-förordningen innebär en inskränkning av innehållsleverantörens yttrandefrihet och användares informationsfrihet. Dessa friheter är dock inte absoluta i regeringsformen utan möjliga att under vissa förutsättningar begränsa genom lag. Den begränsning av ytt-

[22] Prop. 2017/18:174 *En mer heltäckande terrorismlagstiftning*, s. 42 och skäl 22 och artikel 23 i terrorismdirektivet.
[23] Prop. 2009/10:78 *Straffrättsliga åtgärder till förebyggande av terrorism*, s. 29 ff. Se även förslaget om en ny samlad terroristbrottslag i prop. 2021/22:133 *En samlad straffrättslig terrorismlagstiftning.*

rande- och informationsfriheten som TCO-förordningen innebär anser utredningen är motiverad av flera angelägna syften; att skydda Sveriges säkerhet, allmän ordning och säkerhet och att förebygga och beivra brott.

Det undantag som finns i TCO-förordningen för innehåll som sprids i särskilda syften samt det skydd som uttrycks i artikel 1.4 TCO-förordningen innebär, enligt utredningen, att den begränsning av rätten till yttrande- och informationsfrihet som TCO-förordningen innebär inte går utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett åtgärderna.

Bestämmelserna i TCO-förordningen utgör en godtagbar begränsning av yttrande- och informationsfriheten i regeringsformen. Skyddet för yttrande- och informationsfrihet i regeringsformen innebär därför inget hinder mot att tillämpa TCO-förordningen på innehåll som faller utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde men inom regeringsformens skydd för yttrande- och informationsfrihet.

5.6.5 Den behöriga myndighetens prövning

Den ökade användningen av webbsidor, appar, sociala media av såväl traditionella massmedieföretag som av andra aktörer, gör att frågan om huruvida visst innehåll omfattas av yttrandefrihetsgrundlagarna och i vilket syfte en publicering skett kan komma att kräva viss utredning av den behöriga myndigheten.

Den behöriga myndigheten bör utreda syftet med publiceringen för att konstatera om innehållet är undantaget från TCO-förordningens definition av terrorisminnehåll. Om den behöriga myndigheten bedömer att publicering skett i något av de uppräknade syftena är TCO-förordningen inte tillämplig på innehållet och den behöriga myndigheten behöver inte gå vidare i sin bedömning.

Här kan också nämnas att audiovisuella medietjänster är undantagna från TCO-förordningens tillämpningsområde (artikel 1.5 TCO-förordningen). Det innebär att innehåll som sprids i audiovisuella medietjänster inte omfattas av skyldigheterna i TCO-förordningen (se utredningens överväganden i avsnitt 10.4.3).

Om innehållet inte har publicerats med ett godtagbart syfte, och inte i en audiovisuell medietjänst, bör den behöriga myndigheten på

eget initiativ kontrollera om innehållet omfattas av yttrandefrihetsgrundlagarna och särskilt yttrandefrihetsgrundlagen.

Innehåll som publicerats på internet av de traditionella massmedieföretagen dvs. tidningsföretag, programföretag, bokförlag, filmproducenter och nyhetsbyråer får automatiskt grundlagsskydd enligt 1 kap. 4 § yttrandefrihetsgrundlagen och omfattas inte av TCO-förordningen. Det är dock troligt att innehåll som dessa aktörer publicerar på internet faller utanför TCO-förordningens tillämpningsområde redan med hänvisning till syftet med publiceringen. Andra webbsidor kan ha ett utgivningsbevis och därigenom åtnjuta ett frivilligt grundlagsskydd.

Slutligen kan innehåll som är föremål för den behöriga myndighetens prövning omfattas av webbsändningsregeln. Det förslag till författningsändring av webbsändningsregeln som är under beredning kan komma att förenkla bedömningen av innehåll som sprids via webbsändningar. Förslaget innebär att vissa webbsändningar som i dag kommit att omfattas av webbsändningsregeln, i framtiden kommer att falla utanför yttrandefrihetsgrundlagens tillämpningsområde.

Den behöriga myndighetens kontroll av om visst innehåll är grundlagsskyddat kan ske genom att myndigheten undersöker vilken aktör som publicerat innehållet. Myndigheten för press, radio och tv:s tillståndsregister kan här tjäna som viss vägledning. I tillståndsregistret på myndighetens webbsida är aktörer med utgivningsbevis registrerade tillsammans med aktörer som anmält en databas med automatiskt grundlagsskydd samt aktörer som anmält webbsändningar. Tillståndsregistret uppdateras regelbundet. Viss försiktighet bör enligt myndigheten iakttas rörande uppgifterna om registrerade databaser med automatiskt grundlagsskydd. Myndigheten har vid kontroller av registret uppmärksammat att inte alla registrerade databaser uppfyller de formella kraven.

Om det trots gjorda kontroller skulle uppstå gränsdragningsproblematik anser utredningen att skyddet för yttrande- och informationsfriheten bör väga tungt. Här kan erinras om skyldigheten för den behöriga myndigheten att endast vidta åtgärder som är nödvändiga, lämpliga och proportionerliga i ett demokratiskt samhälle, med beaktande av den särskilda vikt som tillmäts yttrande- och informationsfriheten (skäl 10). I en sådan situation menar utredningen att den behöriga myndigheten bör ha utrymme att underlåta att besluta om åtgärder mot det aktuella innehållet.

Skyddet för yttrande- och informationsfrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen kan även få betydelse om 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 i landet. För att undvika att innehåll som publicerats i ett grundlagsskyddat media blir föremål för en avlägsnandeorder bör medlemsstaternas respektive behöriga myndigheter ha utrymme att samverka enligt artikel 14 i TCO-förordningen innan den andra staten beslutar om en avlägsnandeorder. Den svenska behöriga myndigheten kan därigenom informera den utländska motsvarigheten om innebörden av det svenska grundlagsskyddet. För att underlätta samverkan och det gränsöverskridande samarbetet mellan medlemsstaterna ser utredningen fördelar med att Sverige ansluter sig till Europols it-system PERCI.

Skulle en avlägsnandeorder ändå utfärdas i den andra medlemsstaten har den behöriga myndigheten i Sverige under vissa förutsättningar möjlighet att initiera ett granskningsförfarande enligt artikel 4 TCO-förordningen och pröva om ordern är uppenbart oförenlig med TCO-förordningen eller EU:s stadga.

6 En internationell utblick och möjligheten att använda frivilliga åtgärder

6.1 Inledning

I detta kapitel gör utredningen en mindre utblick inom EU och till Storbritannien för att redogöra för hur några länder redan i dag, innan TCO-förordningen börjat tillämpas, arbetar mot spridning av terrorisminnehåll och annat olagligt innehåll på internet.

Inom EU finns sedan 2015 en särskild enhet vid Europol som arbetar mot terrorism- och våldsbejakande extremistiskt innehåll på internet. Enheten – The EU Internet Referral Unit (EU IRU) – identifierar och tar emot information om innehåll på internet som uppfattas strida mot en värdtjänstleverantörs användarvillkor. Om EU IRU bedömer att innehållet strider mot en värdtjänstleverantörs användarvillkor skickar EU IRU en anmälan[1] till den berörda värdtjänstleverantören om att avlägsna innehållet. En värdtjänstleverantör är inte bunden av anmälan utan gör en självständig bedömning av om innehållet strider mot leverantörens användarvillkor och därför bör tas bort. I genomsnitt avlägsnas 86 procent av det material som EU IRU anmäler som oförenligt med en värdtjänstleverantörs användarvillkor.[2]

För svensk rätt är TCO-förordningen och dess skyldigheter ett nytt sätt att arbeta mot att terrorisminnehåll sprids på internet. Sverige arbetar inte sedan tidigare med frivilliga referrals och lämnar inte, såvitt utredningen känner till, information om innehåll på internet till EU IRU. Utredningen återkommer i slutet av avsnittet till möj-

[1] Anmälan och begäran används synonymt i avsnittet. På engelska benämns motsvarande icke rättsligt bindande kontakt; referral.
[2] www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru (hämtad 2022-01-04).

ligheterna för den behöriga myndigheten i Sverige att, parallellt med de rättsligt bindande åtgärderna i TCO-förordningen, även använda sig av frivilliga kontakter med värdtjänstleverantörer, till exempel genom s.k. referrals.

6.2 Danmark

Danmark arbetar redan i dag aktivt mot spridning av terrorisminnehåll på internet. I den danska rättegångsbalken finns en särskild bestämmelse om blockering av webbsidor. Dansk polis kan med stöd av bestämmelsen begära att en domstol ska besluta om blockering av en webbsida om det finns skäl att anta att det via webbsidan begås gärningar som faller in under vissa bestämmelser om terroristbrott i den danska strafflagen (71 kap. 791 d § retsplejeloven).[3]

Danmark har sedan 2017 en nationell Internet Referral Unit (IRU). Enheten är placerad inom den danska säkerhetspolisen, Politiets Efterretningstjeneste (PET). PET ansvarar för terrorbekämpningen i Danmark, varför PET IRU enbart granskar, utifrån säkerhetspolisens ansvarsområde, innehåll som utgör terrorism eller våldsamt extremistiskt innehåll enligt dansk straffrätt. Annat innehåll på internet som utgör till exempel bedrägeri, barnpornografi, upphovsrättsliga överträdelser eller hatbrott tas i stället om hand av den danska polisens nationella cybersäkerhetscenter.

PET IRU:s uppdrag är att identifiera, granska och få bort terrorisminnehåll och våldsamt extremistiskt innehåll från internet. Enheten arbetar uteslutande med förebyggande undersökningar där de aktivt letar efter olagligt innehåll. Den största andelen ärenden som enheten hanterar härrör från enhetens egna undersökningar. En mindre andel härrör från tips som polisen tar emot från allmänheten och vidarebefordrar till enheten.

Merparten av det material som identifieras och granskas av PET IRU påträffas på värdtjänster som är etablerade utanför Danmark och ofta även utanför EU. Om innehåll påträffas på en värdtjänst som är etablerad utanför Danmark skickar PET IRU en informell begäran med information till värdtjänstleverantören om att myndigheten har påträffat innehåll som anses strida mot dansk lag.

[3] https://danskelove.dk/retsplejeloven (hämtad 2022-03-22).

Om terrorisminnehåll eller våldsamt extremistiskt innehåll påträffas hos en dansk värdtjänstleverantör eller enskild person överlämnar PET IRU ärendet till dansk polis för vidare handläggning eftersom enheten saknar rättsligt mandat att inleda en brottsutredning.

Om enheten påträffar en icke-dansk webbsida som har till (enda) syfte att sprida terrorisminnehåll eller våldsamt extremistiskt innehåll, och en begäran inte fått önskad effekt, kan dansk polis använda möjligheten att vända sig till dansk domstol och begära ett domstolsbeslut med krav på att den danska internetleverantören blockerar tillgången till webbsidan i Danmark.

Under de år som enheten har funnits har endast ett ärende rört en dansk värdtjänstleverantör. Enheten har endast påträffat ett fåtal personer i Danmark som spridit den typen av innehåll på internet. Mellan den 1 januari 2018 och den 31 december 2020 har PET IRU handlagt cirka 250 ärenden. Av dessa har 100 ärenden resulterat i att en begäran har skickats till den berörda värdtjänstleverantören.

Vid stickkontroller har myndigheten konstaterat att i hälften av ärendena har allt, eller i vart fall merparten, av det berörda innehållet avlägsnats. Enheten kan dock inte avgöra om innehållet avlägsnats med anledning av PET IRU:s begäran eller om det avlägsnats genom värdtjänstleverantörens egna filter eller efter kontakt med andra myndigheter.

Totalt har PET IRU anmält 42 084 olika innehåll, 35 948 av dessa har avlägsnats av värdtjänstleverantören.

PET IRU:s bedömning efter verksamhetens första år i drift är att begäran, eller s.k. referrals, är ett effektivt verktyg, särskilt i förhållande till de större seriösa värdtjänstleverantörerna.

Här kan även tilläggas att Danmark i samband med att TCO-förordningen antogs utfärdade en särskild deklaration med ett förtydligande att om den danska behöriga myndigheten får information om en order som utfärdats mot en dansk värdtjänstleverantör enligt artikel 4 i TCO-förordningen (en gränsöverskridande order) så ska den danska myndigheten informera värdtjänstleverantören om orderns legala effekt i Danmark.[4]

[4] Declaration by Denmark on the Regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online, Europaudvalget 2020-21, EUU Alm.del Bilag 569, Offentligt, www.ft.dk/samling/20201/almdel/EUU/bilag/ 569/ 2406223.pdf (hämtad 2021-12-20).

6.3 Frankrike

Frankrike har drabbats av flera terrorattentat under senare år vilket bidragit till att landet vidtagit en rad lagstiftningsåtgärder för att förhindra att nya attentat äger rum.

Den franska regeringen utfärdade 2015 ett dekret med en möjlighet att genom ett administrativt förfarande besluta om blockering av webbsidor som innehåller övergrepp mot barn eller terrorism.[5] I en rapport från Commission nationale de l'informatique et des libertés (CNIL, Frankrikes dataskyddsmyndighet) framgår att under perioden januari till december 2020 utfärdades 519 beslut om blockering av webbsidor. Besluten omfattade bland annat 28 webbsidor med terrorisminnehåll.[6]

I maj 2020 antog det franska parlamentet en lag mot hatiskt innehåll på internet.[7] Lagen innebar, på motsvarande sätt som den tyska förebilden NetzDG (se nedan), att stora plattformsföretag ska pröva om innehåll som rapporterats av en användare är olagligt. Om leverantören bedömer att innehållet är uppenbart olagligt ska det avlägsnas inom 24 timmar. Lagen innehöll ursprungligen en skyldighet för en leverantör som mottar en myndighetsorder att inom en timme avlägsna terrorisminnehåll eller barnpornografiskt innehåll som omfattas av ordern. Vid överträdelser av lagen riskerar värdjänstleverantörer böter på upp till 20 miljoner euro eller, i vissa fall, maximalt fyra procent av bolagets globala omsättning. Le Conseil constitutionnel, den högsta franska instans som beslutar i konstitutionella frågor, prövade lagens förenlighet med den franska konstitutionen. Rådet bedömde i ett beslut som meddelades den 18 juni 2020, dvs. innan lagen började tillämpas, att flera bestämmelser inte var förenliga med den franska konstitutionen. Bland annat ansåg rådet att bestämmelserna om avlägsnande av innehåll stred mot rätten till yttrandefrihet.[8] Dessa skyldigheter kom därför aldrig att tillämpas.

I juli 2021 beslutade det franska parlamentet om en lag som rör garantier för respekten för republiken. Lagen innehåller bestämmel-

[5] Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique ; www.legifrance.gouv.fr/loda/id/ JORFTEXT000030195477/ (hämtad 2022-01-12).
[6] Linden, M. Alexandre, "*Rapport d'activité de la personnalité qualifiée 2020*", den 8 juni 2020, www.cnil.fr/sites/default/files/atoms/files/rapport_linden_2020.pdf (hämtad 2022-03-07).
[7] Loi no. 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970 (hämtad 2021-12-22).
[8] www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm (hämtad 2021-12-22).

ser om blockering av spegel-websidor (eng. mirror websites) och bestämmelser om avlägsnande av innehåll på internet som har vissa likheter med de tidigare underkända bestämmelserna.[9]

Utöver dessa lagstiftningsåtgärder är Frankrike även en av två initiativtagare till the Christchurch Call for Action. Ett initiativ som togs efter terrorattentatet mot två moskéer i Christchurch på Nya Zeeland i mars 2019, då ett stort antal människor dödades och skadades. Terrorattentatet livesändes av gärningsmannen och filmen blev snabbt viral. På initiativ av premiärministern i Nya Zeeland och Frankrikes president grundades the Christchruch Call for Action, en frivillig sammanslutning av stater, organisationer och tech-företag som arbetar mot förekomsten av terrorisminnehåll och våldsbejakande extremistiskt innehåll på internet. Många länder och flera stora plattformsföretag har anslutit sig, däribland Sverige.[10]

6.4 Tyskland

Tyskland antog 2017 en lag för att motverka spridning av olagligt innehåll i sociala medier. Lagen; Netzwerkdurchsetzungsgesetz (NetzDG) har till syfte att bekämpa hatbrott, s.k. fake news och annat olagligt innehåll i sociala medier.[11] Redan tidigare fanns en skyldighet för värdtjänster i Telemedia-lagen[12] att avlägsna olagligt innehåll så snart de får kännedom om sådant innehåll.

NetzDG är tillämplig på innehåll i sociala medier som utgör till exempel förolämpning, förtal, offentlig uppmaning till brott, uppvigling till hat, spridning av våldsskildringar och hot om brott. Lagen är tillämplig på sociala medier med mer än två miljoner registrerade användare i Tyskland.

[9] LOI n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République. www.legifrance.gouv.fr/loda/id/JORFTEXT000043964778/?isSuggest=true (hämtad 2022-01-04). Se även beskrivningen på https://freedomhouse.org/country/france/freedom-net/2021#footnote3_4cq6hqi (hämtad 2022-01-04).

[10] www.christchurchcall.com/ (hämtad 2022-01-12). För en mer utförlig beskrivning se utredningens delbetänkande SOU 2021:76 *EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet*, avsnitt 3.3.3.

[11] www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html (hämtad 2021-12-14).

[12] Den tyska Telemedia-lagen från den 26 februari 2007 (Federal Gazette I, p. 179) implementerar bland annat 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”).

Sociala medier definieras i NetzDG som leverantörer av telemediatjänster som i vinstsyfte driver en plattform utformad att göra det möjligt för användare att utbyta och dela innehåll med andra användare eller att göra sådant innehåll tillgängligt för allmänheten.

Vissa leverantörer undantas från lagens tillämpningsområde. Även plattformar med journalistiskt innehåll eller utbildningsinnehåll undantas från tillämpningsområdet. Material kan också undantas när en aktör publicerar (journalistiskt) material på en annan social mediaplattform, till exempel på en Facebooksida. Lagen är inte tillämplig på social media-tjänster som vänder sig till specifika intressegrupper eller specifika ämnen. Det innebär till exempel att affärsnätverk, forum för specialintressen, onlinespel och webbshoppingsidor inte omfattas av lagen.[13]

För leverantörer av sociala medier innebär NetzDG en skyldighet att organisera effektiva och transparanta klagomålsmekanismer på plattformarna. En leverantör måste omedelbart agera och granska ett klagomål för att bedöma om innehållet är olagligt. Om aktören bedömer att innehållet är uppenbart olagligt ska det avlägsnas eller åtkomsten till innehållet blockeras inom tjugofyra timmar från det att värdtjänsten tog emot klagomålet. Annat olagligt innehåll ska avlägsnas eller göras oåtkomligt inom sju dagar, alternativt kan aktören hänskjuta innehållet till ett erkänt institut för bedömning. Skyldigheten att avlägsna olagligt innehåll innebär inte att aktören måste förhandsgranska innehållet på plattformen.

Lagen ger användare rätt att få information om beslut som en aktör meddelat med anledning av ett inlämnat klagomål. Innehåll som avlägsnas ska vidare bevaras av leverantören i tio veckor för eventuell brottsutredning.

Leverantörer av sociala medier ska lämna in transparensrapporter till tyska myndigheter där det ska framgå bland annat hur många klagomål aktören tagit emot.

En aktör som inte uppfyller kraven i NetzDG riskerar höga böter. Den ansvarige för klagomålsfunktionen på ett social media-företag riskerar maximalt 5 miljoner euro i böter och företaget upp till 50 miljoner euro i böter.[14]

[13] www.bmjv.de/SharedDocs/FAQ/EN/NetzDG/NetzDG.html (hämtad 2021-12-14).
[14] www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html (hämtad 2022-01-04).

6.5 Storbritannien

Storbritannien har, likt Frankrike, drabbats av flera terrorattentat under senare år. Landet har antagit ett antal rättsakter för att förhindra nya attentat. Bland annat har *encouragement of terrorism*[15] kriminaliserats i Terrorist Act från 2006. I samma lag kriminaliseras även spridning av publikationer med terrorisminnehåll. Bestämmelserna kan under vissa förutsättningar även tillämpas på innehåll som sprids på internet. [16]

Även Storbritannien har en nationell Internet Referral Unit. Enheten etablerades 2010 och benämns The Counter-Terrorism Internet Referral Unit (CTIRU). Likt andra IRU tar den brittiska enheten emot tips från allmänheten och andra aktörer samt gör egna eftersökningar på internet. Allmänheten kan rapportera misstänkt terrorisminnehåll på internet bland annat genom att använda ett anonymt tips-verktyg på internet.[17]

Om enheten anser att innehåll omfattas av brittisk terrorismlagstiftning skickar enheten en begäran till berörd värdtjänstleverantör. Värdtjänstleverantören bedömer sedan självständigt om innehållet strider mot leverantörens användarvillkor och om det ska avlägsnas.[18]

För närvarande pågår ett lagstiftningsärende rörande en ny lag kallad the Online Safety Bill som har till syfte att bland annat reglera ansvaret för sociala medier-aktörer.[19]

6.6 Utredningens överväganden kring möjligheten att använda frivilliga åtgärder

Utredningens bedömning: Den behöriga myndigheten kan ta informella kontakter med en värdtjänstleverantör vars värdtjänst missbrukas för spridning av terrorisminnehåll.

[15] Motsvarar närmast offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.
[16] Terrorist Act 2006, part 1, section 1-3, www.legislation.gov.uk/ukpga/2006/11/section/1 (hämtad 2022-01-11).
[17] https://act.campaign.gov.uk/ (hämtad 2022-01-11).
[18] www.counterterrorism.police.uk/together-were-tackling-online-terrorism/ (hämtad 2022-01-11).
[19] https://committees.parliament.uk/publications/8206/documents/84092/default/ (hämtad 2022-03-07).

Utredningens arbete och kontakter med representanter för andra medlemsstater leder till slutsatsen att möjligheten att använda ickebindande referrals eller andra informella kontakter med värdtjänstleverantör framstår som ett framgångsrikt sätt att motverka olagligt innehåll på internet.

Det har framkommit att referrals, även när TCO-förordningen börjar tillämpas, fortsatt kommer att vara ett viktigt verktyg i flera medlemsstater, i vissa fall till och med ett förstahandsval. Bland annat har representanter för tyska myndigheter beskrivit ett möjligt scenario där avlägsnandeorder med stöd av TCO-förordningen i framtiden kommer att användas först när en värdtjänstleverantör inte följer en referral eller när det är fråga om en överhängande fara för liv och hälsa.

Även TCO-förordningen uttrycker motsvarande positiva inställning till referrals i skäl 40. Där anges att 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 gör det möjligt för dem att snabbt vidta åtgärder. Anmälningar beskrivs vidare som en mekanism för att uppmärksamma värdtjänstleverantörer på information som skulle kunna anses utgöra terrorisminnehåll, så att de självständigt kan bedöma om det innehållet är förenligt med deras egna användarvillkor. Sådana anmälningar bör förbli tillgängliga vid sidan av avlägsnandeorder.

TCO-förordningen förtydligar även i skäl 40 att förordningen inte bör påverka Europols mandat som fastställs i Europol-förordningen[20]. TCO-förordningen ska därför inte tolkas som att den hindrar medlemsstaterna och Europol från att använda anmälningar som ett verktyg för att uppmärksamma värdtjänstleverantörer på förekomsten av terrorisminnehåll på deras tjänst.

Den digitala plattformen PERCI, som utformas inom Europol för att hantera kommunikation dels mellan medlemsstater, dels mellan medlemsstater och värdtjänstleverantörer inom ramen för TCO-förordningen, kommer även att hantera referrals.

Sverige har inte någon nationell Internet Referral Unit (IRU). Inte heller lämnar någon svensk myndighet information till EU IRU. Så

[20] 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).

vitt framkommit har inte någon svensk myndighet i dag informella kontakter med värdtjänstleverantörer om de påträffar terrorisminnehåll på internet. I utredningsarbetet har det förts diskussioner kring möjligheten för den behöriga myndigheten att, parallellt med TCO-förordningen och i likhet med flera andra medlemsstater, använda sig av informella kontakter med värdtjänstleverantörer. Det har därvid från berörda myndigheter framförts en tvekan kring om det verktyget bör användas utan lagstöd eller i vart fall utan ett uttryckligt uppdrag.

Att närmare överväga och föreslå en nationell IRU faller utanför utredningens uppdrag. Utredningen kan emellertid se fördelar med att inrätta en nationell Internet Referral Unit för att förhindra spridning av olagligt innehåll på internet, så som terrorisminnehåll.

Det är därtill utredningens uppfattning att det inte finns något som hindrar att myndigheten som utses till behörig myndighet redan i samband med ikraftträdandet av TCO-förordningen kan ta informella kontakter med värdtjänstleverantörer. Som framgått ovan framhåller förordningen fördelarna med referrals och uttrycker även att TCO-förordningen inte hindrar en fortsatt användning av referrals. Den behöriga myndigheten bör därför ha möjlighet att när terrorisminnehåll som omfattas av TCO-förordningen påträffas på internet ta kontakt med värdtjänstleverantören och informera denne om förekomsten av terrorisminnehållet.

Innehåll som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen omfattas inte av TCO-förordningen (se avsnitt 5.6). Den behöriga myndigheten bör därför inte ta kontakt med en värdtjänstleverantör om det aktuella innehållet bedöms vara grundlagsskyddat.

En informell kontakt skulle i många situationer kunna framstå som en mer proportionerlig och lämplig åtgärd jämfört med att utfärda en rättsligt bindande avlägsnandeorder. Den behöriga myndigheten bör i det enskilda fallet alltid göra en bedömning av om det är lämpligt med en informell kontakt med den berörda värdtjänstleverantören. Om myndigheten tar kontakt är det av vikt att myndigheten inte formulerar sig på ett sådant sätt att åtgärden uppfattas som tvingande av värdtjänstleverantören.

Om det är fråga om en värdtjänstleverantör som inte vidtar åtgärder mot spridning av terrorisminnehåll eller om det är fråga om ett överhängande hot mot liv och hälsa (jfr artikel 14.5 TCO-förordningen) bör avlägsnandeorder användas i första hand.

7 Allmänna överväganden

7.1 En ny lag ska komplettera TCO-förordningen

Utredningens bedömning: En ny lag med bestämmelser som kompletterar TCO-förordningen ska införas.

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

Hänvisningar till TCO-förordningen i kompletteringslagen ska, med undantag för bestämmelserna om förelägganden och sanktionsavgifter, vara dynamiska, dvs. avse förordningen i den vid varje tidpunkt gällande lydelsen.

En EU-förordning är, i enlighet med artikel 288 andra stycket i Fördraget om EU:s funktionssätt, till alla delar bindande och direkt tillämplig i varje medlemsstat. Till skillnad från ett direktiv får en förordning inte införlivas i eller omvandlas till nationell rätt. Det innebär att medlemsstaterna är förhindrade att utfärda bestämmelser i frågor som regleras i en förordning. Medlemsstaterna får inte uttala sig om tillämpningen av en förordning eller förtydliga innebörden av begrepp som förekommer i en förordning. Tolkningen av en förordning är förbehållet de myndigheter och domstolar som tillämpar förordningen i respektive medlemsstat. I sista hand är det EU-domstolen som har tolkningsrätt över en EU-förordning.

Normalt behöver inte de enskilda medlemsstaterna införa kompletterande nationella bestämmelser till en EU-förordning. Det kan dock bli aktuellt om en EU-förordning överlämnar vissa frågor åt medlemsstaterna att reglera. Medlemsstaterna har även en skyldighet att se till att en EU-förordning kan tillämpas i praktiken och får ett effektivt genomslag i medlemsstaten. I många fall förutsätter en EU-förordning därför att medlemsstaterna inför nationella regler av verkställande karaktär.

TCO-förordningen överlämnar vissa frågor till medlemsstaterna att reglera. Det handlar främst om vilken myndighet som ska vara behörig myndighet, vilka sanktioner som ska aktualiseras vid överträdelser av förordningen och att medlemsstaterna säkerställer rätten till effektiva rättsmedel. Dessa frågor utgör kärnan i utredningens uppdrag.

De nationella bestämmelser som ska komplettera TCO-förordningen bör föras in i en ny lag. För att förtydliga att lagen inte är heltäckande, utan endast ett komplement till TCO-förordningen, bör den nya lagen benämnas lagen med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll på internet. I fortsättningen kallas den nya lagen kompletteringslagen.

Hänvisningsteknik

Kompletteringslagen ska läsas tillsammans med TCO-förordningen. För att undvika dubbelreglering i TCO-förordningen och kompletteringslagen är det lämpligt att hänvisa till förordningen i kompletteringslagen. Den nya lagen med kompletterande bestämmelser innehåller därför hänvisningar till bestämmelser i TCO-förordningen.

Det finns två sätt att hänvisa till unionslagstiftning i nationell rätt, antingen genom statiska hänvisningar eller dynamiska hänvisningar. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En följd av denna hänvisningsteknik är att den nationella författningen normalt behöver ändras varje gång EU-bestämmelsen ändras. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen.

Gröna boken, Riktlinjer för författningsskrivning (Ds 2014:1) rekommenderar att hänvisningar till EU-förordningar, till exempel vid införande av sanktionsbestämmelser, som utgångspunkt bör ske genom statisk hänvisningsteknik. I vissa fall kan det finnas skäl att använda en annan hänvisningsteknik. En upplysningsbestämmelse som inte tillför lagtexten något materiellt innehåll behöver inte innehålla en hänvisning som anger vilken lydelse av rättsakten som avses.

Lagrådet har i ett yttrande uttryckt att det från en konstitutionell utgångspunkt inte synes föreligga något hinder mot att lagstiftaren väljer en teknik för hänvisning till EU-rättsakter som, utan ytterligare lagstiftning, omfattar också eventuella ändringar av rättsakten,

dvs. en dynamisk hänvisningsteknik. Statiska hänvisningar kan, enligt Lagrådet, leda till oklarheter eller brister i lagstiftningen om lagstiftaren inte uppdaterar en hänvisning och medföra behov av att ändra en lag endast för att en hänvisning ska uppdateras utan att några överväganden i sak aktualiseras. Lagrådet anser därför att det kan finnas anledning att i vissa fall välja en dynamisk hänvisningsteknik. För att komma fram till vilken teknik som är lämplig i det enskilda fallet rekommenderar Lagrådet att lagstiftaren gör en konsekvensanalys som redovisas i anslutning till varje bestämmelse. Konsekvensanalysen bör bland annat innehålla en redogörelse över hur det nationella regelsystemet ändras genom hänvisningen och hur ändringar av rättsakten kan komma att påverka den nationella regleringen.[1]

En dynamisk hänvisningsteknik är även det sätt som förordats av regeringen i flera lagstiftningsärenden under senare år.[2]

Kompletteringslagen kommer att innehålla vissa hänvisningar till TCO-förordningen. Det är lämpligast att som utgångspunkt använda en dynamisk hänvisningsteknik eftersom eventuella framtida ändringar i TCO-förordningen därigenom får direkt genomslag i nationell rätt.

Hänvisning till bestämmelser av upplysande karaktär bör vara dynamiska för att undvika oklarheter.

Vid utformningen av ett nationellt sanktionssystem krävs det i princip en fullständig nationell reglering. För att en värdtjänstleverantör ska kunna förutse vilka sanktioner som kan bli följden av en överträdelse bör hänvisningar till TCO-förordningen i bestämmelserna om sanktioner ske med statiska hänvisningar.

Termer och uttryck

Flera av de termer och uttryck som används i TCO-förordningen definieras i artikel 2 TCO-förordningen. Termer och uttryck som används i kompletteringslagen bör ha samma betydelse som i TCO-förordningen. Utredningen föreslår därför att lagen upplysningsvis ska innehålla en hänvisning till TCO-förordningen för betydelsen av de termer och uttryck som används i lagen.

[1] Yttrande från Lagrådet, utdrag ur protokoll från sammanträde 2016-03-15.
[2] Se till exempel prop. 2017/18:105 *Ny dataskyddslag*, s. 24 f. och prop. 2018/19:26 *Kompletterande bestämmelser till EU:s geoblockeringsförordning*, s. 18–19.

7.2 Behovet av andra författningsändringar

Utredningens bedömning: För att säkerställa att TCO-förordningen får ett effektivt genomslag i svensk rätt och undvika dubbelreglering behöver utredningen överväga författningsändringar i BBS-lagen, e-handelslagen och radio- och tv-lagen.

Det finns även anledning att överväga om det finns behov av tillägg eller ändringar i offentlighets- och sekretesslagen och dataskyddslagstiftningen.

Det ingår i utredningens uppdrag att analysera om det finns behov av att ändra lagen (1998:112) om ansvar för elektroniska anslagstavlor (BBS-lagen). BBS-lagen har vissa beröringspunkter med TCO-förordningen, särskilt när det kommer till bestämmelsen i 5 § om att ta bort ett meddelande eller på annat sätt förhindra vidare spridning av ett meddelande. 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 meddelandets innehåll uppenbart är sådant som avses i bestämmelserna om till exempel uppvigling i 16 kap. 5 § brottsbalken, hets mot folkgrupp i 16 kap. 8 § brottsbalken, olaga våldsskildring i 16 kap. 10 c § brottsbalken, offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen)[3]. BBS-lagens och TCO-förordningens tillämpningsområde sammanfaller i viss utsträckning. Det finns därför anledning för utredningen att överväga ändringar av BBS-lagen.

I e-handelslagen, som implementerar e-handelsdirektivet i svensk rätt, finns särskilda bestämmelser som reglerar vissa fall av ansvarsfrihet för olagligt innehåll som sprids på en värdtjänstleverantörs värdtjänst. Även här finns det anledning för utredningen att närmare analysera förhållandet mellan e-handelslagen och TCO-förordningen.

Både radio- och tv-lagen (2010:696) och TCO-förordningen innehåller skyldigheter för vissa aktörer att förhindra spridning av innehåll med offentlig uppmaning till terroristbrott respektive terrorisminnehåll. Det finns därför anledning för utredningen att även överväga hur bestämmelserna i radio- och tv-lagen, särskilt beträffande leve-

[3] Se författningsförslagen i prop. 2021/22:133 *En samlad straffrättslig terrorismlagstiftning*, s. 9 f. och s. 23.

rantörer av videodelningsplattformar, förhåller sig till TCO-förordningen.

I utredningens uppdrag ingår även att föreslå de författningsändringar och andra åtgärder som behövs för att den behöriga myndigheten ska kunna tillämpa TCO-förordningen och vidta de åtgärder som ankommer på myndigheten på ett effektivt och rättssäkert sätt. I delbetänkandet föreslog utredningen att Polismyndigheten bör utses till behörig myndighet och att Polismyndigheten i sitt uppdrag kan behöva inhämta information och kunskap från till exempel Säkerhetspolisen, Totalförsvarets forskningsinstitut eller Centrum mot våldsbejakande extremism vid Brottsförebyggande rådet. Den behöriga myndighetens handläggning av TCO-ärenden och samverkan med dessa myndigheter väcker frågor om sekretess och personuppgiftsbehandling. Det finns därför även ett behov av att överväga ändringar i offentlighets- och sekretesslagen (2009:400) och dataskyddslagstiftningen.

7.3 Rätten att överklaga ett beslut enligt TCO-förordningen och kompletteringslagen

Utredningens förslag: Beslut som den behöriga myndigheten meddelar med stöd av TCO-förordningen och kompletteringslagen ska kunna överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

TCO-förordningen överlämnar till varje enskild medlemsstat att införa effektiva förfaranden för utövandet av rätten till effektiva rättsmedel (artikel 9 TCO-förordningen).

I TCO-förordningen framgår att värdtjänstleverantörer som mottagit en avlägsnandeorder som utfärdats enligt artikel 3.1 eller ett beslut som meddelats enligt artikel 4.4, artiklarna 5.4, 5.6 eller 5.7 ska ha rätt till ett effektivt rättsmedel. Denna rätt ska innefatta rätten att bestrida en avlägsnandeorder inför domstolarna i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern och rätten att bestrida beslut enligt artikel 4.4, artiklarna 5.4, 5.6 eller 5.7 inför domstolarna i den medlemsstat vars behöriga myndighet meddelade beslutet.

Även innehållsleverantörer ska enligt TCO-förordningen ges en rätt till effektiva rättsmedel i vissa fall. En innehållsleverantör 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 inför domstolarna i den medlemsstat vars behöriga myndighet utfärdade ordern och rätten att bestrida ett beslut enligt artikel 4.4 inför domstolarna i den medlemsstat vars behöriga myndighet fattade beslutet.

Värdtjänstleverantörer och innehållsleverantörer ska i den utsträckning som framgått ovan ha rätt till effektiva rättsmedel. Rätten gäller oberoende av om leverantörerna är enskilda personer eller juridiska personer.

Utgångspunkten är att rätten till ett effektivt rättsmedel mot myndighetsbeslut uppnås genom möjligheten att överklaga ett beslut till allmän förvaltningsdomstol (40 § förvaltningslagen [2017:900]). Detsamma gäller beslut som fattas med stöd av en EU-förordning. Utredningen ser ingen anledning att frångå gängse sätt och föreslår därför att beslut som den behöriga myndigheten meddelar med stöd av TCO-förordningen och kompletteringslagen ska få överklagas till allmän förvaltningsdomstol. En särskild bestämmelse om överklagande bör införas i kompletteringslagen.

Utredningens förslag är sammanfattningsvis att värdtjänstleverantörer och innehållsleverantörer får överklaga ett beslut som meddelats av den behöriga myndigheten till allmän förvaltningsdomstol, vilket i första instans är förvaltningsrätten. Ett överklagande ska göras skriftligen till förvaltningsrätten men ges in till den behöriga myndigheten. För prövning i nästa instans av kammarrätt ska det krävas prövningstillstånd (se 40 § förvaltningslagen).

Utredningen föreslår i avsnitt 8.5 ett sanktionssystem i svensk rätt vid överträdelser av TCO-förordningen. I avsnittet redogör utredningen för rätten till effektiva rättsmedel vid beslut om sanktioner som meddelas av den behöriga myndigheten.

Genom möjligheten att överklaga beslut som den behöriga myndigheten meddelar med stöd av TCO-förordningen och kompletteringslagen till domstol säkerställs rätten till effektiva rättsmedel i svensk rätt.

7.4 Ikraftträdande

TCO-förordningen ska tillämpas i alla medlemsstater från och med den 7 juni 2022. Kompletteringslagen och de ändringar i svensk rätt som utredningen föreslår bör träda i kraft samtidigt och så snart som möjligt. Utredningens bedömning är att det med hänsyn till remissförfarandet och övriga beredningsåtgärder inte är möjligt att låta författningsförslagen träda i kraft förrän den 1 juli 2023.

8 Sanktionssystemet

8.1 Utgångspunkter i TCO-förordningen

En sanktion är en bred beskrivning av en påföljd vid ett olagligt handlande som antingen kan ha ett handlingsdirigerande eller ett bestraffande syfte. En sanktion kan vara en straffrättslig påföljd eller administrativ påföljd så som sanktionsavgift, vite, förbud eller återkallelse av tillstånd.

Så som utredningen beskrivit tidigare överlåter TCO-förordningen till medlemsstaterna att fastställa nationella regler om sanktioner vid överträdelser av förordningen. Det åligger medlemsstaterna att vidta alla åtgärder som krävs för att säkerställa att det nationella sanktionssystemet tillämpas (artikel 18 och skäl 45). Sanktionerna – som kan vara av administrativ eller straffrättslig art – ska vara *effektiva, proportionella och avskräckande*. Vilka överträdelser som kan föranleda en sanktion framgår av en uppräkning i artikel 18.

En behörig myndighet i respektive medlemsstat ska ha befogenhet att besluta om sanktioner. Medlemsstaterna ska säkerställa att den behöriga myndigheten beaktar alla relevanta omständigheter, inklusive de som följer av artikel 18.2, när myndigheten beslutar om en sanktion och fastställer sanktionens typ och nivå.

Medlemsstaterna ska vidare säkerställa att en värdtjänstleverantör som systematiskt eller fortgående underlåter att fullgöra skyldigheterna i artikel 3.3 får böter på upp till fyra procent av leverantörens totala omsättning under det föregående räkenskapsåret.

Ordalydelsen i artikel 18 innebär inte att det enbart är aktuellt med straffrättsliga böter. Böter i TCO-förordningens mening kan även avse administrativa sanktioner, jfr engelska textens ”*financial penalties*”.

Utredningens uppdrag består i denna del av att kartlägga vilka sanktioner som skulle kunna aktualiseras vid ett åsidosättande av

skyldigheterna i TCO-förordningen och föreslå hur ett nationellt sanktionssystem bör se ut.

Kapitlet inleds med en redogörelse för de möjliga sanktioner som finns i svensk rätt. De administrativa sanktionerna förbud och återkallelse av tillstånd är inte aktuella vid överträdelser av TCO-förordningen. Utredningen berör därför inte dessa sanktioner närmare nedan. Den avslutande delen av kapitlet innehåller utredningens överväganden och förslag till ett nationellt sanktionssystem.

8.2 Kriminalisering av överträdelser

Straffrättsliga påföljder finns i brottsbalken och i ett stort antal lagar inom specialstraffrätten. Vad som är straffrättsliga påföljder följer av 1 kap. 3 § brottsbalken. Där framgår det att med påföljd för brott avses straffen böter och fängelse samt villkorlig dom, skyddstillsyn och överlämnande till särskild vård.

Straff som påföljd vid lagöverträdelser är det mest ingripande och långtgående verktyg som samhället har för att styra dess medborgares beteende i en viss riktning.

Kriminalisering uttrycks ofta som en *ultima ratio*, en sista utväg, och bör därför som regel användas med försiktighet av lagstiftaren.[1] Om det finns någon alternativ sanktion som är tillräckligt effektiv och mindre ingripande bör den väljas i stället. Lagstiftaren har återkommit till denna försiktighetsprincip vid flera tillfällen, till exempel i prop. 1994/95:23 *Ett effektivare brottmålsförfarande* (s. 52):

> Kriminalisering som en metod för att söka hindra överträdelse av olika normer i samhället bör användas med försiktighet. Rättsväsendet bör inte belastas med sådant som har ringa eller inget straffvärde. Kriminalisering är heller inte det enda och inte alltid det mest effektiva medlet för att motverka oönskade beteenden. Det allmännas resurser för brottsbekämpning bör koncentreras på sådana förfaranden som kan föranleda påtaglig skada eller fara och som inte kan bemötas på annat sätt.

Kriminalisering av överträdelser är dessutom kostsamt och tidskrävande för samhället, särskilt rättsväsendet. Frågor om avkriminalisering och sanktionsväxling har varit föremål för diskussion och även genomförts i svensk lagstiftning.[2] En sanktionsväxling innebär att

[1] Asp, P. och Ulväng, M. *Kriminalrättens grunder*, (2013, version 2, JUNO), s. 32 ff.
[2] Se till exempel prop. 1994/95:23 *Ett effektivare brottmålsförfarande* och SOU 2013:38 *Vad bör straffas?*

lagstiftning som tidigare var kriminaliserad avkriminaliseras och att det i stället införs administrativa sanktioner, till exempel sanktionsavgifter, för att motverka det oönskade beteendet.

Straffrättsanvändningsutredningen fick till uppgift att bland annat ta ställning till om vissa oönskade beteenden kan mötas mer effektivt genom andra former av sanktioner eller åtgärder än straff och att analysera, samt ta ställning till, vilka kriterier som bör gälla för att kriminalisering ska anses vara lämplig.[3] Utredningen föreslog i betänkandet *Vad bör straffas?* (SOU 2013:38) fem kriterier att beakta vid överväganden av om en överträdelse ska kriminaliseras eller om det är tillräckligt ingripande med andra administrativa sanktioner:[4]

1. Det tänkta straffbudet måste avse ett identifierat och konkretiserat intresse som är skyddsvärt (godtagbart skyddsintresse).
2. Det beteende som avses bli kriminaliserat måste kunna orsaka skada eller fara för skada på ett skyddsintresse.
3. Endast den som visat skuld – varit klandervärd – bör träffas av straffansvar, vilket innebär att kriminaliseringen inte får äventyra tillämpningen av skuldprincipen.
4. Det får inte finnas något tillräckligt värdefullt motstående intresse.
5. Det får inte finnas någon alternativ metod som är tillräckligt effektiv för att komma till rätta med det oönskade beteendet. Här kan följande beaktas:
   - Finns det redan en handlingsdirigerande regel som är tillräckligt effektiv för att motverka det oönskade beteendet?
   - Om en handlingsdirigerande regel behöver införas – kan beteendet motverkas tillräckligt effektivt med en regel som inte är repressiv, till exempel en civilrättslig regel om skadestånd?
   - Om det är nödvändigt att införa en repressiv handlingsdirigerande regel för att motverka det oönskade beteendet ska lagstiftaren i första hand välja vite, sanktionsavgift eller återkallelse av tillstånd och straff i sista hand.

[3] Kommittédirektiven 2011:31 *Användningen av straffrätt*.
[4] SOU 2013:38 s. 19–20.

En i sammanhanget viktig skillnad, jämfört med administrativa sanktioner, är att straffansvar endast kan träffa fysiska personer.

En juridisk person kan visserligen bli föremål för en talan om företagsbot. En företagsbot är dock inte ett straff utan en särskild rättsverkan av brott. För att åläggas företagsbot krävs det att ett brott har begåtts. Det innebär att såväl subjektiva som objektiva rekvisit ska vara uppfyllda. En gärningsman behöver inte identifieras eller åtalas, men en företagsbot förutsätter i praktiken att det går att identifiera en fysisk person i den juridiska personen för att visa att de subjektiva rekvisiten är uppfyllda.[5]

Även inom EU har Europaparlamentet, likt den svenska lagstiftaren, uttryckt en försiktighet inför att kriminalisera överträdelser av unionslagstiftning. I en straffrättslig strategi från 2012 uttalas att kriminalisering ska användas som en sista utväg för att hantera ett tydligt fastställt och avgränsat beteende som inte kan hanteras effektivt genom mindre stränga åtgärder och som orsakar samhället eller individer betydande skada. En gärning bör annorlunda uttryckt kriminaliseras endast om mindre ingripande åtgärder är otillräckliga för att skydda ett viktigt allmänt och grundläggande intresse.[6]

8.3 Vitesföreläggande

Ett föreläggande som förenas med vite (vitesföreläggande) är en administrativ sanktion som har ett preventivt syfte för att på förhand få mottagaren att vidta vissa handlingar. Vitet som sanktion är därför handlingsdirigerande, till skillnad från sanktionsavgifter och straffrättsliga påföljder som är tillbakaverkande eftersom de aktualiseras först när en överträdelse har ägt rum. Både fysiska och juridiska personer kan få ett vitesföreläggande.

Föreläggande om vite och utdömande av vite regleras i lagen (1985:206) om viten (viteslagen). Viteslagen innehåller huvudsakligen bestämmelser som reglerar individuella viten. Individuella viten kan vara antingen förfarandeviten eller materiella viten. Förfarandeviten kan beskrivas som viten som syftar till att påverka mottagaren att

[5] Johannisson, Brottsbalk (1962:700) 36 kap. 7 § brottsbalken, Lexino 2021-08-01 (JUNO).
[6] Europaparlamentets resolution av den 22 maj 2012 om en straffrättslig strategi inom EU (2010/2310(INI)) punkten I.

vidta en viss handling. Materiella viten är i stället viten som avser att framtvinga iakttagande av slutliga beslut.[7]

Ett vite som föreläggs enligt 3 § viteslagen ska vara bestämt till ett visst belopp. Beloppet ska fastställas med hänsyn till vad som är känt om mottagarens ekonomiska förhållanden och omständigheter i övrigt som kan antas förmå mottagaren att följa föreläggandet. Med omständigheterna i övrigt avses bland annat kostnaderna och omfattningen av åtgärderna som mottagaren måste vidta för att följa föreläggandet. Beloppet bör också bestämmas med hänsyn till hur angeläget det är att mottagaren följer föreläggandet. Om föreläggandet avser att tillgodose ett betydelsefullt samhällsintresse, till exempel upprättande av allmän ordning och säkerhet, kan ett högt belopp vara motiverat.[8]

Ett vite kan även föreläggas som löpande vite om det är lämpligt med hänsyn till omständigheterna. Ett löpande vite innebär att vitet bestäms till ett visst belopp för varje tidsperiod av viss längd under vilken föreläggandet inte har följts eller, om föreläggandet avser en återkommande förpliktelse, för varje gång mottagaren underlåter att fullgöra förpliktelsen (4 §).

Utgångspunkten är att vite inte kan föreläggas när straff är utsatt. Straff bör här ges en vidare definition än den som följer av brottsbalken och snarare motsvara begreppen *påföljd* eller *sanktion*. För att utnyttja de olika fördelarna med vite och straff har rättsutvecklingen gått mot lagstiftning som anger att vite får sättas ut även om straff är stadgat, men att om det sker så får straff inte dömas ut. I till exempel 9 kap. 7 § strålskyddslagen (2018:396) framgår att den som har åsidosatt ett vitesföreläggande inte ska dömas till ansvar enligt strålskyddslagen för en gärning som omfattas av föreläggandet. På detta sätt får beslutsmyndigheten möjlighet att välja mellan vite och straff och mottagaren riskerar inte att drabbas av dubbla sanktioner. För att bestämmelsen ska vara tillämplig krävs dock gärningsidentitet. Det innebär att den straffbelagda gärningen måste vara identisk, både i tid och rum och riktas mot samma person, med den gärning som innebär att ett vite döms ut enligt ett vitesföreläggande.[9]

[7] Lavin, R. Viteslagstiftningen, kommentaren till 1 § viteslagen, version 3B, 2019-12-02 (JUNO).
[8] Lavin, R. Viteslagstiftningen, kommentaren till 3 § viteslagen, version 3B, 2019-12-02 (JUNO).
[9] Lavin, R. Viteslagstiftningen, kommentaren till 2 § viteslagen, version 3B, 2019-12-02 (JUNO).

Både sanktionsavgifter och utdömande av viten är att betrakta som straff i Europakonventionens mening.[10] Högsta domstolen har i rättsfallet NJA 2013 s. 502 uttalat att inte enbart ett slutligt avgörande utgör ett hinder mot att inleda ett andra förfarande. Även en pågående prövning är ett hinder mot ett nytt förfarande. Det avgörande för när ett hinder mot ett andra förfarande uppkommer är tidpunkten när domstolsprocessen inleds. När det kommer till vitesföreläggande blir den avgörande tidpunkten när en ansökan om utdömande av vite görs.

Bestämmelser om föreläggande som får förenas med vite finns bland annat i 17 kap. 11 § radio- och tv-lagen (2010:696). Genom radio- och tv-lagen kan Myndigheten för press, radio och tv till exempel förelägga en aktör att lämna vissa upplysningar eller årlig redovisning. Myndigheten kan också besluta om de förelägganden som behövs för att få leverantörer av videodelningsplattformar att vidta lämpliga åtgärder enligt 9 a kap. 1 § och 3 § (se vidare i avsnitt 10.4).

Det har framförts viss kritik mot vitesförelägganden. Vitets effektivitet som sanktion har ifrågasatts främst eftersom tidsutdräkten innan vitet i praktiken ska betalas kan bli lång om mottagaren överklagar både beslutet om föreläggande och beslutet om utdömande av vitet.[11]

8.4 Sanktionsavgifter

8.4.1 Inledning

En sanktionsavgift är, likt vitesförelägganden, en administrativ sanktion som kan påföras både fysiska och juridiska personer.[12] En sanktionsavgift kan antingen beslutas av förvaltningsmyndighet eller av domstol och tillfaller normalt staten.

Bestämmelser om sanktionsavgifter införs vanligtvis i syfte att verka avskräckande och bestraffande eftersom en sanktionsavgift kan bli aktuell först när en överträdelse har ägt rum. Sanktionsavgifter är därför inte, så som vitesföreläggande, handlingsdirigerande.

[10] Se beträffande viten till exempel prop. 2012/13:143 *Effektivare sanktioner för arbetsmiljö- och arbetstidsreglerna*, s. 69 och prop. 2020/21:186 *Kompletterande bestämmelser till EU:s cybersäkerhetsakt*, s. 41.
[11] Se till exempel prop. 2007/08:107 *Administrativa sanktioner på yrkesfiskets område*, s. 15.
[12] Warnling Conradson, W och Nilsson A., *Sanktionsavgifter – Särskilt i näringsverksamhet*, version 2, 2020 (JUNO), s. 44.

En sanktionsavgift är inte en straffrättslig påföljd. Det finns dock vissa likheter med straff som gör att sanktionsavgifter rättsligt har en ställning mellan avgifter och straffrättsliga påföljder. En sanktionsavgift är att betrakta som ett straff i Europakonventionens mening.[13] Ett sanktionsavgiftsförfarande ska därför uppfylla de rättigheter och skyldigheter som följer av Europakonventionen. Det innebär att mottagaren, den som påstås ha överträtt en bestämmelse, till exempel har rätt att underrättas om vad som läggs denne till last, rätt att yttra sig över anklagelsen och rätt till domstolsprövning inom rimlig tid. I svensk rätt följer rätten till domstolsprövning av förvaltningslagen (2017:900) där det i 4 § och 40 § framgår att ett beslut av en förvaltningsmyndighet kan överklagas till förvaltningsdomstol om inte annat följer av annan lagstiftning.

Antalet författningar som innehåller bestämmelser om sanktionsavgifter har ökat över tid. Inledningsvis berodde ökningen på sanktionsväxling från straff (för lindrigare brottslighet) till sanktionsavgifter. Under senare år har sanktionsavgifter ofta införts i svensk rätt vid överträdelser av unionslagstiftning, se till exempel lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt, lagen (2019:59) med kompletterande bestämmelser till EU:s geoblockeringsförordning och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Ytterligare en anledning till ökningen av antalet bestämmelser om sanktionsavgifter har varit lagstiftarens önskan att införa sanktioner mot juridiska personer. Eftersom endast fysiska personer kan bli föremål för straffrättsliga påföljder anses sanktionsavgifter ofta vara ett effektivt redskap för att komma åt överträdelser som begås i näringsverksamhet.

8.4.2 Utformning av bestämmelser om sanktionsavgifter

Utgångspunkten är att bestämmelser om sanktionsavgifter ska, på motsvarande sätt som vid straffrättsliga påföljder, utformas med beaktande av ett antal rättssäkerhetsprinciper. Till exempel ska det enkelt gå att utläsa vilken gärning som kan föranleda en sanktionsavgift,

[13] Till exempel prop. 2012/13:143 *Effektivare sanktioner för arbetsmiljö- och arbetstidsreglerna*, s. 71 f. och Warnling Conradson, W och Nilsson A., *Sanktionsavgifter – Särskilt i näringsverksamhet* s. 18.

vem bestämmelsen riktar sig mot (mottagaren) och hur stor avgift som mottagaren riskerar.

Bestämmelser om sanktionsavgifter har varierande utformning i svensk rätt. Det saknas ett enhetligt system för utformning och tillämpning av sanktionsavgifter. En förklaring till skillnaderna är att många sanktionsavgifter har införts med utgångspunkt i den materiella rättens särskilda behov och syfte. Det finns därför sanktionsavgifter som riktar sig mot fysiska eller juridiska personer. Ett antal sanktionsavgifter kan beslutas av en förvaltningsmyndighet som första instans, andra beslutas av domstol (se även nedan om sanktionsavgiftsföreläggande). I de flesta sanktionsavgiftssystem är dock beslutanderätten placerad nära den myndighet som har bäst kunskap om det materiella regelverket. Det innebär att det normalt är den berörda tillsynsmyndigheten som beslutar om sanktionsavgifter. Att ge tillsynsmyndigheten beslutanderätt har bland annat i förarbetena till 2018 års spellag beskrivits som det mest lämpliga ur resursanvändningsperspektiv.[14]

Andra skillnader mellan sanktionsavgiftssystemen är sättet att bestämma avgiftens storlek. Storleken kan bestämmas utifrån en på förhand fastställd avgift (schablon) eller en avgift som är beroende av en viss variabel.[15] Vid utformningen av bestämmelser om sanktionsavgifter som riktar sig mot juridiska personer kan lagstiftaren använda vinsteliminerande sanktionsavgifter, i motsats till på förhand bestämda belopp, för att uppnå god styreffekt. Genom att koppla avgiftens storlek till näringsidkarens årsomsättning eller hämta ledning från reglerna om företagsbot, skapas vinsteliminerande och avskräckande sanktionsavgifter.[16]

Även om det inte alltid framgår av lagtexten så bygger ofta bestämmelser om sanktionsavgift på ett strikt ansvar.[17] Det innebär att en mottagare inte behöver ha haft uppsåt eller varit oaktsam för att åläggas en sanktionsavgift. Prövningsmyndighetens bedömning blir på detta sätt enklare och mer effektiv eftersom myndigheten inte behöver göra de svåra bedömningar som i många fall krävs vid prövning av subjektiva rekvisit.

[14] Prop. 2017/18:220 *En omreglerad spelmarknad*, s. 233.
[15] SOU 2013:38 *Vad bör straffas?* s. 467 f.
[16] SOU 2013:38 s. 544.
[17] Se Lagrådets yttrande i prop. 2012/13:55 *En ny lag om kontroll av ekologisk produktion*, s. 142.

8.4.3 Särskilt om sanktionsavgiftsföreläggande

Viss kritik har riktats mot sanktionsavgiftssystem eftersom rättssäkerheten i vissa fall anses få stå tillbaka för kravet på effektivitet. Det har till exempel ifrågasatts om det är lämpligt att en administrativ myndighet beslutar i ärenden där avgifterna ibland kan bli mycket höga.[18]

För att bibehålla systemets effektivitet och samtidigt upprätthålla rättssäkerheten och de krav som följer av EKMR har det inom några rättsområden införts ett system med sanktionsavgiftsföreläggande. Ett sanktionsavgiftsföreläggande innebär att den administrativa myndigheten förelägger mottagaren att betala en sanktionsavgift. Mottagaren kan välja att godkänna föreläggandet vilket får till följd att föreläggandet blir en verkställbar exekutionstitel. Om mottagaren motsätter sig att betala avgiften blir ärendet tvistigt och den administrativa myndigheten kan ansöka vid allmän förvaltningsdomstol om att avgiften ska utgå. Den administrativa myndigheten blir då part i ärendet vid domstolen.[19]

Bland annat inom arbetsmiljörätten används ett system med sanktionsavgiftsföreläggande. Där finns i åttonde kapitlet arbetsmiljölagen (1977:1160) en möjlighet för regeringen, eller den myndighet regeringen bestämmer (Arbetsmiljöverket), att föreskriva om sanktionsavgifter för vissa typer av överträdelser mot arbetsmiljölagen och även ett system med sanktionsavgiftsföreläggande. Om mottagaren av ett sanktionsavgiftsföreläggande bestrider ett föreläggande om sanktionsavgift kan Arbetsmiljöverket ansöka vid allmän förvaltningsdomstol om att avgiften ska påföras av domstolen (8 kap. 5–10 §§ arbetsmiljölagen).

8.5 Utredningens överväganden och förslag

8.5.1 Inledning

Utredningen har ovan redogjort för vilka sanktioner som finns i svensk rätt och som utredningen kan överväga vid utformningen av ett nationellt sanktionssystem. I detta avsnitt överväger utredningen

[18] Prop. 2014/15:57 *Nya administrativa sanktioner på finansmarknadsområdet*, s. 56 ff.
[19] Warnling Conradson, W. och Nilsson, A., *Sanktionsavgifter – Särskilt i näringsverksamhet*, version 2, 2020 (JUNO), s. 109 ff.

alternativen och föreslår ett nationellt sanktionssystem vid överträdelser av TCO-förordningen.

Det framgår av TCO-förordningen att sanktionerna ska vara effektiva, proportionella och avskräckande. Förordningen överlämnar dock till de enskilda medlemsstaterna att avgöra om sanktionerna ska vara straffrättsliga eller administrativa. Några andra riktlinjer kring vilka sanktioner som medlemsstaterna bör överväga framgår inte av förordningen.

En viktig utgångspunkt när utredningen överväger ett sanktionssystem är att TCO-förordningens materiella bestämmelser är tillämplig på alla aktörer – såväl fysiska som juridiska personer – som omfattas av begreppet värdtjänstleverantör i artikel 2 i TCO-förordningen. Sanktionssystemet bör därför vara effektivt, proportionerligt och avskräckande gentemot både fysiska och juridiska personer.

8.5.2 Överträdelser ska inte vara straffsanktionerade

Utredningens bedömning: Överträdelser av TCO-förordningen ska inte vara straffsanktionerade.

De artiklar i TCO-förordningen som ska förenas med sanktioner innehåller skyldigheter som åläggs värdtjänstleverantörer. Det är således värdtjänstleverantörer, vilket kan vara både fysiska och juridiska personer, som kan bli föremål för de sanktioner utredningen nu ska föreslå. Även om en fysisk person kan omfattas av begreppet värdtjänstleverantör är det utredningens uppfattning att merparten av de berörda värdtjänstleverantörerna är juridiska personer. Det är därför viktigt att de sanktioner som utredningen föreslår är effektiva i förhållande till juridiska personer.

Juridiska personer kan inte åläggas straffansvar. En kriminalisering av överträdelser av TCO-förordningen skulle därför inte verka avskräckande för merparten av de värdtjänstleverantörer som är skyldiga att följa bestämmelserna i TCO-förordningen. Redan av den anledningen framstår inte straff som en lämplig sanktion.

Juridiska personer kan visserligen bli föremål för talan om företagsbot (36 kap. 7 § brottsbalken). En förutsättning för ansvar är dock att brottet har begåtts i utövningen av företagets verksamhet vilket kan innebära bevissvårigheter. Även ur denna aspekt framstår krimi-

nalisering som ett mindre effektivt styrmedel vid överträdelser av TCO-förordningen.

Utredningens bedömning är att kriminalisering inte är ett effektivt verktyg vid överträdelser av TCO-förordningen. Utredningen föreslår således inte några straffbestämmelser.

I sammanhanget kan tilläggas att TCO-förordningen innehåller åtgärder som ska motverka att värdtjänster missbrukas för spridning av terrorisminnehåll på internet. Förordningen varken utesluter eller hindrar att en innehållsleverantör, dvs. den som tillhandahållit innehållet som spridits på värdtjänsten, eller annan, blir föremål för straffrättsliga påföljder med stöd av till exempel rekryteringslagen.[20]

8.5.3 Överträdelser ska leda till administrativa sanktioner

Utredningens förslag: Överträdelser av TCO-förordningen ska leda till administrativa sanktioner.

Beslut om vitesföreläggande och sanktionsavgift är lämpliga sanktioner vid överträdelser av TCO-förordningen.

Utredningen har i det förra avsnittet gjort bedömningen att överträdelser av TCO-förordningen inte bör kriminaliseras. Det alternativ som återstår att överväga är därmed administrativa sanktioner.

Utredningen ser flera fördelar med att välja administrativa sanktioner vid genomförandet av TCO-förordningen. Administrativa sanktioner kan riktas mot både fysiska och juridiska personer. Förfarandet är snabbt och effektivt. Den ekonomiska avgiften kan sättas högt (eller lågt) och göras beroende av vilken skyldighet aktören åsidosatt och vilken aktör som ska påföras sanktionen.

Det är utredningens bedömning att administrativa sanktioner kan utgöra ett effektivt och avskräckande styrmedel gentemot både fysiska och juridiska personer, oavsett verksamhetens storlek. Det är också vanligt att administrativa sanktioner införs i svensk rätt för att genomföra och komplettera rättsakter från EU.

I svensk rätt är vitesföreläggande, sanktionsavgift, återkallelse av tillstånd och förbud möjliga administrativa sanktioner. Återkallelse av tillstånd och förbud saknar här relevans med hänsyn till hur TCO-

[20] Se prop. 2021/22:133 *En samlad straffrättslig terrorismlagstiftning* där de nationella straffrättsliga bestämmelserna om terrorismrelaterad brottslighet föreslås samlas i en ny terroristbrottslag.

förordningen är utformad. De administrativa sanktioner som återstår att överväga är därmed *beslut om vitesförelägganden* och *sanktionsavgifter*.

Som framgått är skyldigheterna som åläggs värdtjänstleverantörer i TCO-förordningen av mycket olika slag. Flera artiklar i förordningen innehåller skyldigheter för värdtjänstleverantörer att vidta åtgärder för att utforma sina värdtjänster så att förekomsten av terrorisminnehåll motverkas. Om en värdtjänstleverantör underlåter att uppfylla dessa krav behöver medlemsstaterna ett effektivt verktyg som verkar handlingsdirigerade, för att få till stånd TCO-förordningens övergripande syfte – att motverka förekomsten av terrorisminnehåll på internet. Utredningen föreslår därför att den behöriga myndigheten bör få möjlighet att förelägga en värdtjänstleverantör att vidta åtgärder så att leverantören uppfyller kraven i TCO-förordningen. Ett sådant föreläggande ska kunna förenas med vite.

Ett vitesföreläggande är inte lämpligt vid alla former av överträdelser av TCO-förordningen. Om en värdtjänstleverantör inte följer en avlägsnandeorder är ett vitesföreläggande mindre verkningsfullt. En handlingsdirigerande sanktion är inte effektiv eftersom en överträdelse redan har ägt rum. Den formen av åsidosättanden bör i stället föranleda en sanktion med ett bestraffande syfte. En sanktionsavgift är då en mer lämplig sanktion.

Utredningens uppfattning är att det nationella sanktionssystemet vid överträdelser av TCO-förordningen bör bestå av administrativa sanktioner, dels genom bestämmelser om föreläggande som kan förenas med vite, dels genom bestämmelser om sanktionsavgifter. Sanktionssystemet bör föras in i kompletteringslagen.

Vilken sanktion som är lämplig i det enskilda fallet är beroende av vilken form av åsidosättande det är fråga om. I nästa avsnitt redogör utredningen för i vilka situationer det är lämpligt med vitesförelägganden respektive sanktionsavgifter.

8.5.4 Vitesföreläggande vid handlingsdirigerande bestämmelser

Utredningens förslag: Den behöriga myndigheten ska kunna besluta om förelägganden mot en värdtjänstleverantör som åsidosätter sina skyldigheter enligt TCO-förordningen, i dess ursprungliga lydelse, att inom viss tid vidta en viss åtgärd. Det handlar om skyldigheter att:

- utse eller inrätta en kontaktpunkt för mottagande av avlägsnandeorder (artikel 15.1 TCO-förordningen),
- utforma sina användarvillkor så att de uppfyller kraven i artikel 5.1 och 7.1 i TCO-förordningen,
- vidta specifika åtgärder som uppfyller kraven i artikel 5.2 och 5.3 i TCO-förordningen,
- inrätta klagomålsmekanismer enligt artikel 10.1 i TCO-förordningen,
- granska klagomål som lämnats in till värdtjänstleverantören enligt artikel 10.2 i TCO-förordningen,
- lämna in en rapport till den behöriga myndigheten enligt artikel 5.5 i TCO-förordningen,
- lämna in en transparensrapport enligt artikel 7.2 och 7.3 i TCO-förordningen, och
- utse en fysisk eller juridisk person till rättslig företrädare enligt kraven i artikel 17 i TCO-förordningen.

Den behöriga myndigheten ska ges möjlighet att förena ett föreläggande med vite.

Gemensamt för de skyldigheter som utredningen redogör för i detta avsnitt är att sanktionen vid en överträdelse bör vara handlingsdirigerande. Detta för att skapa ett incitament för värdtjänstleverantörer att vidta de åtgärder som TCO-förordningen kräver och därigenom motverka spridning av terrorisminnehåll på den berörda värdtjänsten.

Möjligheten att utfärda en avlägsnandeorder mot terrorisminnehåll på internet är TCO-förordningens mest kraftfulla verktyg mot spridning av terrorisminnehåll. Systemet bygger på att värdtjänst-

leverantörer utser eller inrättar en kontaktpunkt som kan ta emot och skyndsamt handlägga en avlägsnandeorder (artikel 15.1). Det är därför av stor vikt att en sådan kontaktpunkt inrättas så att den behöriga myndigheten snabbt kan komma i kontakt med en värdtjänstleverantör. Av den anledningen bör den behöriga myndigheten ges möjlighet att besluta om föreläggande mot en värdtjänstleverantör som åsidosätter sin skyldighet att utse eller inrätta en kontaktpunkt. Ett sådant föreläggande ska kunna förenas med vite.

Andra skyldigheter i TCO-förordningen syftar till att få värdtjänstleverantörer, främst de som anses exponerade för terrorisminnehåll, att utforma sina värdtjänster på ett sådant sätt att möjligheten att de missbrukas för att sprida terrorisminnehåll motverkas.

En värdtjänstleverantör ska alltid klart och tydligt i *användarvillkoren* ange sin strategi för att åtgärda spridning av terrorisminnehåll och, när det är lämpligt, förklara hur åtgärderna fungerar (artikel 7.1). En värdtjänstleverantör som anses exponerad för terrorisminnehåll ska därutöver, i tillämpliga fall, i sina användarvillkor inkludera och tillämpa bestämmelser om åtgärder mot spridning av terrorisminnehåll (artikel 5.1). Det är utredningens uppfattning att även i dessa situationer är det lämpligt att ge den behöriga myndigheten möjlighet att utfärda ett föreläggande mot en värdtjänstleverantör, som kan förenas med vite, med krav på att aktören utformar sina användarvillkor i enlighet med skyldigheterna i TCO-förordningen.

En värdtjänstleverantör som är exponerad för terrorisminnehåll ska även vidta *specifika åtgärder* för att skydda sin värdtjänst mot spridning av terrorisminnehåll (artikel 5.2). En värdtjänstleverantör bestämmer själv vilka åtgärder som ska vidtas men åtgärderna ska uppfylla de krav som framgår av artikel 5.3. För att säkerställa att en värdtjänstleverantör vidtar nödvändiga åtgärder och att åtgärderna uppfyller kraven i artikel 5.2 och 5.3 bör den behöriga myndigheten även här ges möjlighet att vitesförelägga en värdtjänstleverantör att vidta specifika åtgärder som uppfyller förordningens krav.

Artikel 5.6 är utformad på ett annat sätt än de övriga artiklar som räknas upp i artikel 18. Av artikel 5.6 följer att den behöriga myndigheten ska rikta ett föreläggande mot en värdtjänstleverantör som inte uppfyller kraven i artikel 5.2 och 5.3. Bestämmelsen riktar sig således till den behöriga myndigheten men ska enligt artikel 18 förenas med en sanktion. Utredningen har ovan föreslagit att vid en underlåtenhet att uppfylla kraven i artikel 5.2 och 5.3 ska den behö-

riga myndigheten ha möjligheten att utfärda ett vitesföreläggande med direkt stöd av artikel 5.2 och 5.3. Det saknas därför behov av att även föreslå en sanktion som kopplas till artikel 5.6.

Till skyldigheten att vidta specifika åtgärder följer även en *rapporteringsskyldighet* i artikel 5.5. En värdtjänstleverantör som mottar ett beslut om exponering ska inom tre månader, och därefter årligen, rapportera till den behöriga myndigheten vilka åtgärder som har vidtagits och vidtas. Ytterligare ett transparenskrav finns i artikel 7.2 och 7.3 och innebär att en värdtjänstleverantör som vidtagit åtgärder för att förhindra spridning av terrorisminnehåll eller ålagts att vidta åtgärder enligt förordningen, ska offentliggöra en transparensrapport över det gångna årets åtgärder. Rapporten ska offentliggöras senast den 1 mars följande år. En överträdelse av skyldigheterna i artikel 5.5 och 7.2–7.3 är förhanden först när tidsfristerna i respektive bestämmelse har passerat. Behovet av transparens i värdtjänstleverantörernas strategier för terrorisminnehåll är avgörande för att öka leverantörers ansvar gentemot användare och stärka medborgarnas förtroende för den digitala inre marknaden (skäl 30). För att säkerställa att värdtjänstleverantörer uppfyller TCO-förordningens krav på transparens och faktiskt upprättar och offentliggör rapporter, är det mest lämpligt att även här ge den behöriga myndigheten en möjlighet att besluta om vitesföreläggande.

Slutligen bör den behöriga myndigheten ges möjlighet att vitesförelägga en värdtjänstleverantör som är exponerad för terrorisminnehåll att inrätta *klagomålsmekanismer* som gör det möjligt för en innehållsleverantör att lämna in klagomål mot innehåll som avlägsnats eller gjorts oåtkomligt och begära att innehållet återställs (artikel 10.1). Vidare bör den behöriga myndigheten ha möjlighet att vitesförelägga en värdtjänstleverantör som inte granskar inlämnade klagomål enligt kraven i artikel 10.2 TCO-förordningen.

Värdtjänstleverantörer utanför EU

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

företrädare med de befogenheter och resurser som krävs för att följa avlägsnandeorder och beslut och i övrigt samarbeta med de behöriga myndigheterna. Den rättsliga företrädaren ska vara bosatt eller etablerad i en medlemsstat där värdtjänstleverantören erbjuder sina tjänster (artikel 17.1 och 17.2 TCO-förordningen).

Den rättsliga företrädaren ska kunna hållas ansvarig för överträdelser av TCO-förordningen, utan att det påverkar värdtjänstleverantörens eventuella ansvar eller eventuella rättsliga åtgärder mot denne (artikel 17.3 TCO-förordningen).

Värdtjänstleverantören ska underrätta den behöriga myndigheten i den medlemsstat där dess rättsliga företrädare är bosatt eller etablerad om vem som är rättslig företrädare. Informationen om den rättsliga företrädaren ska offentliggöras av värdtjänstleverantören.

Om en värdtjänstleverantör inte uppfyller dessa skyldigheter bör den behöriga myndigheten ha möjlighet att besluta om ett vitesföreläggande.

8.5.5 Vitets storlek

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

När den beslutande myndigheten ska fastställa storleken på ett vite ska myndigheten beakta de omständigheter som följer av artikel 18.2:

a) överträdelsens karaktär, allvar och varaktighet,

b) om överträdelsen var avsiktlig eller orsakades av vårdslöshet,

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

d) värdtjänstleverantörens finansiella styrka,

e) graden av tjänsteleverantörens samarbete med de behöriga myndigheterna,

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

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

Uppräkningen i artikel 18.2 är inte uttömmande, i artikeln används ordet ”inbegripet”.

Det bör framgå av kompletteringslagen att dessa omständigheter ska beaktas när storleken på vitet fastställs.

8.5.6 Handläggning av ärenden om vitesföreläggande

Utredningens bedömning: Ett ärende om vitesföreläggande ska handläggas enligt viteslagen (1985:206), förvaltningslagen (2017:900) och förvaltningsprocesslagen (1971:291).

Beslut om föreläggande ska kunna förenas med vite i de fall som utredningen redogjort för ovan. Ett sådant beslut fattas av den behöriga myndighet som regeringen utser enligt 3 § kompletteringslagen.

Om en värdtjänstleverantör inte följer ett vitesföreläggande kan den behöriga myndigheten enligt 6 § viteslagen ansöka om vitets utdömande vid förvaltningsdomstol (se vidare i viteslagen).

Ett ärende om vitesföreläggande och utdömande av vite ska handläggas enligt viteslagen, förvaltningslagen (1 §) och förvaltningsprocesslagen.

8.5.7 Överträdelser som kan leda till sanktionsavgift

Utredningens förslag: Den behöriga myndigheten ska ges möjlighet att besluta om sanktionsavgifter mot en värdtjänstleverantör som åsidosätter sina skyldigheter enligt TCO-förordningen, i dess ursprungliga lydelse, genom

– 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),

- underlåtenhet att utan onödigt dröjsmål informera den behöriga myndigheten om att terrorisminnehåll har avlägsnats eller att terrorisminnehåll gjorts oåtkomligt i samtliga medlemsstater med angivelse av i synnerhet vid vilken tidpunkt innehållet avlägsnades eller gjordes oåtkomligt (artikel 3.6 TCO-förordningen),
- underlåtenhet att enligt artikel 4.7 i TCO-förordningen omedelbart återställa avlägsnat innehåll eller åtkomsten till det,
- underlåtenhet att bevara terrorisminnehåll som avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder eller specifika åtgärder enligt artikel 6 i TCO-förordningen,
- underlåtenhet att informera berörd innehållsleverantör att innehåll avlägsnats eller gjorts oåtkomligt enligt artikel 11.1–11.2 i TCO-förordningen,
- att lämna ut information i strid med artikel 11.3 i TCO-förordningen, och
- underlåtenhet att underrätta berörd brottsutredande myndighet om att värdtjänstleverantören fått kännedom om terrorisminnehåll som innebär ett överhängande hot mot en eller flera personers liv (artikel 14.5 TCO-förordningen).

Flera skyldigheter i TCO-förordningen är av sådan karaktär att ett åsidosättande bör föranleda en bestraffande sanktion. Eftersom en sanktionsavgift är tillbakaverkande och kan användas först när en överträdelse har ägt rum är sanktionsavgifter en lämplig sanktion i sådana situationer.

Möjligheten att utfärda avlägsnandeorder är ett av huvudverktygen i TCO-förordningen för att motverka spridning av terrorisminnehåll på internet. En överträdelse av artikel 3.3 och 4.2 bör leda till en sanktion med ett i första hand bestraffande syfte. Om den behöriga myndigheten kan konstatera att en värdtjänstleverantör som mottagit en avlägsnandeorder i enlighet med artikel 3, inte avlägsnat eller gjort terrorisminnehållet oåtkomligt i alla medlemsstater bör den behöriga myndigheten ges möjlighet att besluta om en sanktionsavgift.

Utöver skyldigheten att ta bort eller göra terrorisminnehåll oåtkomligt till följd av en order följer det även en informationsskyldig-

het i artikel 3.6 och 11. En värdtjänstleverantörs underlåtenhet att utan dröjsmål informera den behöriga myndigheten enligt artikel 3.6 att terrorisminnehållet avlägsnats eller gjorts oåtkomligt med angivelse av i synnerhet tidpunkten för avlägsnandet, bör också kunna föranleda en sanktionsavgift. Det samma gäller skyldigheten att informera en innehållsleverantör om att berört innehåll avlägsnats eller gjorts oåtkomligt samt, om en innehållsleverantör begär det, skälen för avlägsnandet (artikel 11). I artikel 11.3 finns även en möjlighet för den behöriga myndigheten att besluta att skälen för en avlägsnandeorder inte får lämnas ut. En värdtjänstleverantör som i strid med ett sådant beslut ändå lämnar ut informationen bör också kunna påföras en sanktionsavgift.

En värdtjänstleverantör är även, på det sätt som framgår av artikel 6, skyldig att bevara terrorisminnehåll som avlägsnats eller gjorts oåtkomligt med anledning av en avlägsnandeorder eller specifika åtgärder samt därtill hörande data som avlägsnats till följd av att terrorisminnehållet avlägsnats. Kan den behöriga myndigheten konstatera att en värdtjänstleverantör inte bevarat terrorisminnehåll enligt artikel 6 bör ett sådant åsidosättande av förordningen också kunna leda till en sanktionsavgift.

En värdtjänstleverantör som får ett beslut om oförenlighet ska omedelbart återställa det avlägsnade innehållet eller åtkomsten till det (artikel 4.7). Underlåter värdtjänsteleverantören att återställa innehållet anser utredningen att det också är en överträdelse som bör kunna föranleda en sanktionsavgift.

Slutligen ska en värdtjänstleverantör, vid äventyr av att en sanktion annars kan påföras, underrätta brottsutredande myndigheter i berörd medlemsstat om värdtjänstleverantören får kännedom om innehåll som medför ett överhängande hot mot en eller flera personers liv (jfr engelska textens *imminent threath to life*) (artikel 14.5). En underlåtenhet att underrätta myndigheterna bör kunna föranleda en sanktionsavgift.

8.5.8 Skyldigheten att betala en sanktionsavgift ska bygga på ett strikt ansvar

Utredningens bedömning: Skyldigheten att betala en sanktionsavgift ska bygga på ett strikt ansvar.

Bestämmelser om sanktionsavgifter bygger ofta på ett strikt ansvar. Det innebär att den behöriga myndigheten inte behöver ta ställning till om ett visst handlande varit uppsåtligt eller oaktsamt. Genom att göra den juridiska prövningen oberoende av subjektiva rekvisit blir den rättsliga bedömningen enklare och mer effektiv.

En ordning med sanktionsavgifter som bygger på ett strikt ansvar bidrar till ett effektivt sanktionssystem vid överträdelser av TCO-förordningen. Utredningen anser därför att bestämmelserna om sanktionsavgifter i kompletteringslagen bör bygga på ett strikt ansvar. Därigenom blir det tillräckligt för den beslutande myndigheten att konstatera att en överträdelse har ägt rum för att en sanktionsavgift ska utgå. Det strikta ansvaret behöver inte framgå uttryckligen av bestämmelserna i kompletteringslagen.

8.5.9 Sanktionsavgiftens storlek

Utredningens förslag: En sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 5 miljoner kronor.

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

Det övergripande syftet med TCO-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 därigenom bidra till den allmänna säkerheten i hela unionen.

När utredningen överväger sanktionsavgiftens storlek är utgångspunkten att en sanktionsavgift ska vara effektiv, proportionerlig och avskräckande för såväl fysiska som juridiska personer.

Utredningen har tidigare konstaterat att de aktörer som kommer omfattas av begreppet värdtjänstleverantör kan vara fysiska personer men att berörda värdtjänstleverantörer huvudsakligen kommer att vara juridiska personer. Värdtjänstleverantörer som är juridiska personer kan skilja sig markant från varandra både i fråga om storlek och ekonomiska förutsättningar. Det är därför viktigt att en sanktionsavgift blir kännbar för både en fysisk person, ett mindre företag med små resurser och ett större företag med stora resurser.

En bestämmelse som reglerar en sanktionsavgifts storlek kan utformas på flera sätt. Den kan ange ett bestämt belopp, ett beloppsintervall (som gäller oavsett vem som begått överträdelsen) eller kopplas till omsättningen i en näringsverksamhet.

För att en sanktionsavgift ska vara effektiv, proportionerlig och avskräckande i förhållande till varje möjlig värdtjänstleverantör anser utredningen att det är mest lämpligt att föreslå ett beloppsintervall.

De överträdelser av TCO-förordningen som utredningen föreslår ska kunna leda till en sanktionsavgift är av varierande art och karaktär. Beloppsintervallet bör därför vara förhållandevis stort för att ge den behöriga myndigheten ett vitt utrymme att göra en nyanserad bedömning av avgiftens storlek i det enskilda fallet.

En avgift som kan bestämmas till lägst 5 000 kronor ger den beslutande myndigheten utrymme att beakta överträdelsens karaktär och allvar men även en värdtjänstleverantörs ekonomiska förmåga. Avgiftens storlek bör kunna sättas högt i det enskilda fallet för att skapa en avskräckande effekt även för värdtjänstleverantörer med stora ekonomiska resurser och därigenom bidra till att TCO-förordningens syfte uppnås. Utredningen föreslår därför att en sanktionsavgift ska kunna bestämmas till lägst 5 000 kronor och högst 5 miljoner kronor.

Vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna i artikel 3.3 (avlägsnandeorder) ska en sanktionsavgift, utan hinder av det ovan föreslagna beloppsintervallet, bestämmas till högst fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret (artikel 18.3).

8.5.10 Sanktionsavgift i det enskilda fallet

Utredningens förslag: När sanktionsavgiftens storlek ska bestämmas i det enskilda fallet ska hänsyn tas till de omständigheter som räknas upp i artikel 18.2 i TCO-förordningen.

Förordningen räknar upp ett antal omständigheter i artikel 18.2 som den beslutande myndigheten ska beakta vid beslut om en sanktions typ och nivå. Uppräkningen, som inte är uttömmande (artikeln använder begreppet inbegripet), omfattar 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 tjänsteleverantörens samarbete med de behöriga myndigheterna,

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

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

Utredningen har ovan föreslagit att bestämmelserna om sanktionsavgift ska bygga på ett strikt ansvar. Utifrån uppräkningen i artikel 18.2 TCO-förordningen finns det utrymme när storleken bestäms att beakta till exempel om en värdtjänstleverantör har begått en uppsåtlig eller oaktsam överträdelse eller om det annars framstår som oskäligt att ta ut full avgift.

8.5.11 Förfarandebestämmelser

Utredningens förslag: Den behöriga myndighet som regeringen bestämmer enligt 3 § kompletteringslagen ska ges möjlighet att besluta om sanktionsavgifter.

Ett beslut om sanktionsavgift ska delges.

En sanktionsavgift får inte beslutas om den som anspråket riktas mot inte har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

En sanktionsavgift ska betalas till den behöriga myndighet som regeringen bestämmer enligt 3 § kompletteringslagen 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 denna tid, ska myndigheten lämna den

obetalda avgiften för indrivning. Vid indrivning får verkställighet ske enligt utsökningsbalken.

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

Sanktionsavgiften ska tillfalla staten.

Beslut om sanktionsavgift ska fattas av den behöriga myndighet som regeringen bestämmer med stöd av 3 § kompletteringslagen.

Ett beslut om sanktionsavgift är en ingripande åtgärd varför ett sådant beslut bör delges den betalningsskyldige värdtjänstleverantören enligt delgivningslagen (2010:1932).

Det är inte lämpligt att meddela ett beslut om sanktionsavgift om lång tid har förflutit sedan överträdelsen ägde rum. Utredningen föreslår därför att en sanktion inte får tas ut om den värdtjänstleverantör som anspråket riktar sig mot inte har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Det är också lämpligt att föreslå en bortre preskriptionstid. Utredningen anser att avgiften bör preskriberas om verkställighet inte skett inom fem år.

Det framgår inte av TCO-förordningen om administrativa sanktioner ska betalas till EU eller till medlemsstaterna. Det saknas även bestämmelser i förordningen om hur de ekonomiska sanktionerna ska betalas eller hur verkställighet ska ske. I avsaknad av närmare reglering i TCO-förordningen bör det framgå av kompletteringslagen att sanktionsavgifter ska tillfalla staten.

Det bör också framgå att en sanktionsavgift ska betalas till den behöriga myndighet som regeringen bestämmer med stöd av 3 § kompletteringslagen 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.[21]

Om en sanktionsavgift inte betalas inom den angivna tiden, ska myndigheten lämna den obetalda avgiften för indrivning. Det bör framgå av kompletteringslagen att vid indrivning får verkställighet ske enligt utsökningsbalken (1981:774). En sanktionsavgift bör falla bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet fick laga kraft.

[21] Jfr prop. 2018/19:26 *Kompletterande bestämmelser till EU:s geoblockeringsförordning*, s. 30.

8.5.12 Förbudet mot dubbelbestraffning

Utredningens bedömning: Eftersom det uttryckligen framgår av kompletteringslagen när en värdtjänstleverantör kan vitesföreläggas respektive påföras sanktionsavgift behövs inte en särskild bestämmelse i kompletteringslagen som förtydligar förbudet mot dubbelbestraffning.

Rätten att inte blir lagförd eller straffad två gånger regleras i artikel 4 i Europakonventionens sjunde tilläggsprotokoll (även kallad principen om *ne bis in idem*). Eftersom Sverige har anslutit sig till tilläggsprotokollet gäller det som lag i Sverige.

Både sanktionsavgift och utdömande av vite är att betrakta som straff i Europakonventionens mening.

Högsta domstolen har i NJA 2013 s. 502 uttalat att ett slutligt avgörande inte ensamt utgör ett hinder mot ett andra förfarande. Även en pågående prövning utgör ett hinder mot att inleda ett nytt förfarande. Det avgörande för när ett hinder mot ett andra förfarande uppkommer är den tidpunkt när domstolsprocessen inleds, dvs. i förhållande till vitesföreläggande när en ansökan om vitets utdömande ges in till domstol.[22]

Dubbelbestraffningsförbudet hindrar således både ett andra straff och en andra prövning av samma gärning. Utgångspunkten vid tillämpningen av kompletteringslagen är att det inte bör uppstå en situation där både sanktionsavgift och vitesföreläggande aktualiseras, eftersom kompletteringslagen föreslås reglera uttryckligen i vilka situationer vitesföreläggande respektive sanktionsavgift kan bli aktuellt. Någon särskild bestämmelse som förtydligar förbudet mot dubbelbestraffning behövs därför inte.

En värdtjänstleverantör kan bli föremål för en straffrättslig process med anledning av det innehåll som sprids på en värdtjänst, till exempel genom ett medverkansbrott eller möjligen som gärningsman.[23] Förbudet mot dubbelbestraffning i tilläggsprotokollet hindrar att en värdtjänstleverantör lagförs två gånger för samma gärning. Gränsdragningsfrågor i detta avseende bör enligt utredningens upp-

[22] Jfr Europadomstolens dom i mål *Muslija mot Bosnien-Herzegovina*, no. 32042/11, den 14 januari 2014.
[23] Se Högsta domstolens resonemang i NJA 2007 s. 805 och Ulväng, M. och Asp, P., *Kriminalrättens grunder*, version 2, 2013 (JUNO), s. 109 ff.

fattning överlämnas till rättstillämpningen. Någon särskild bestämmelse därom föreslås därför inte i kompletteringslagen.

8.5.13 Överklaganden

Utredningens förslag: Den behöriga myndighetens beslut om sanktioner enligt TCO-förordningen och kompletteringslagen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Myndighetsbeslut överklagas normalt till allmän förvaltningsdomstol. Rätten till domstolsprövning av en förvaltningsmyndighets beslut följer av förvaltningslagen (2017:900). Där framgår det i 4 § och 40 § att ett beslut av förvaltningsmyndighet kan överklagas till förvaltningsdomstol om inte annat följer av annan lagstiftning.

Den myndighet som regeringen utser till behörig myndighet för Sveriges räkning kommer att besluta om sanktioner. Beslut om sanktioner ska kunna överklagas av den värdtjänstleverantör som berörs av beslutet.

Utredningens förslag innefattar enbart administrativa sanktioner. Detta talar för att beslut bör överklagas till allmän förvaltningsdomstol. Vissa bedömningar som den behöriga myndigheten kan komma att ställas inför, till exempel om visst innehåll utgör terrorisminnehåll, angränsar till straffrätten. Dessa beröringspunkter utgör enligt utredningens uppfattning inte tillräckliga skäl att frångå den sedvanliga prövningsordningen.

Utredningen föreslår därför att beslut om vitesföreläggande och sanktionsavgifter ska kunna överklagas till allmän förvaltningsdomstol.

Förvaltningsrättens beslut får överklagas till kammarrätten. Det ska krävas prövningstillstånd vid överklagande till kammarrätten. Kammarrättens beslut får överklagas till Högsta förvaltningsdomstolen (33 § förvaltningsprocesslagen).

Utredningen har tidigare berört rätten att överklaga andra beslut som den behöriga myndigheten kan meddela med stöd av TCO-förordningen, se avsnitt 7.3.

9 Sekretess och informationsutbyte

9.1 Inledning

En del av utredningens uppdrag är att överväga vilka författningsändringar och andra åtgärder som krävs för att den behöriga myndigheten ska kunna tillämpa TCO-förordningen och vidta de åtgärder som ankommer på myndigheten på ett effektivt och rättssäkert sätt. Utredningens förslag ska utformas så att den behöriga myndighetens administrativa börda inte ökar mer än nödvändigt.

Utredningen har, som tidigare nämnts, i ett delbetänkande föreslagit att Polismyndigheten bör utses till behörig myndighet enligt TCO-förordningen. Den behöriga myndigheten kommer inom ramen för sitt uppdrag att hantera en mängd olika slags uppgifter. Det finns inte någon bestämmelse i TCO-förordningen som särskilt reglerar sekretess, vare sig som riktar sig till medlemsstaterna eller specifikt till de behöriga myndigheterna.

För en effektiv tillämpning av TCO-förordningen är det utredningens uppfattning att den behöriga myndigheten kommer att behöva samverka och samarbeta på ett europeiskt plan med behöriga myndigheter i andra medlemsstater och Europol, men även med andra nationella myndigheter.

Beträffande samarbetet mellan behöriga myndigheter i andra medlemsstater och Europol innehåller TCO-förordningen i artikel 14 en bestämmelse som innebär att de behöriga myndigheterna ska utbyta information, samordna sig med och samarbeta med varandra och, när så är lämpligt, med Europol för att undvika dubbelarbete, förbättra samordningen och undvika att störa utredningar i andra medlemsstater.

Samverkan med andra nationella myndigheter kan bli aktuellt till exempel om Polismyndigheten ser ett behov av att inhämta underlag

till stöd för bedömningen av om visst innehåll ska anses vara terrorisminnehåll.

Säkerhetspolisen har det nationella uppdraget att förebygga, förhindra och upptäcka terrorismrelaterad brottslighet (3 § polislagen [1984:387]). Säkerhetspolisen har särskild kunskap och erfarenhet av tillämpningen av lagstiftningen på området och de straffrättsliga bedömningar som följer därav. Säkerhetspolisen har även kunskap och kompetens om terrororganisationer samt dessas närvaro och spridning av information på internet. Det är därför troligt att nationell samverkan främst kommer att vara aktuell mellan Polismyndigheten och Säkerhetspolisen. Även andra myndigheter med särskild kunskap om terrorism, till exempel Totalförsvarets forskningsinstitut (FOI) och Centrum mot våldbejakande extremism (CVE) vid Brottsförebyggande rådet, kan också vara aktuella för Polismyndigheten att samverka med.

För att samverkan ska fungera mellan myndigheterna måste det finnas rättsliga förutsättningar att utbyta information. För det krävs dels att informationen inte omfattas av sekretess, alternativt att sekretessen kan brytas, dels att det inte finns något som hindrar behandlingen av personuppgifter.

I detta kapitel redogör utredningen övergripande för den rättsliga regleringen av offentlighet och sekretess samt samverkan och informationsutbyte mellan myndigheter, med särskilt fokus på förutsättningarna för ett effektivt utbyte mellan Polismyndigheten och Säkerhetspolisen. Utredningen överväger först om det finns behov av att föreslå en sekretessbestämmelse som skyddar uppgifter i ett TCO-ärende hos Polismyndigheten. Därefter analyserar utredningen behovet av en sekretessbrytande bestämmelse eller en bestämmelse om uppgiftsskyldighet för att säkerställa ett effektivt och rättssäkert informationsutbyte mellan Polismyndigheten och Säkerhetspolisen. Avslutningsvis berör utredningen behovet av kompletterande bestämmelser i dataskyddslagstiftningen.

Utredningen utgår i analysen från att Polismyndighetens handläggning av ärenden enligt TCO-förordningen och kompletteringslagen inte är en del av Polismyndighetens brottsbekämpande verksamhet. TCO-ärenden kommer att hanteras som administrativa ärenden inom myndigheten vilket får betydelse för vilka sekretess- och dataskyddsbestämmelser som blir tillämpliga.

9.2 Offentlighet och sekretess

9.2.1 Allmänna utgångspunkter

För att främja ett fritt meningsutbyte, en fri och allsidig upplysning och ett fritt konstnärligt skapande har alla och en var rätt att ta del av allmänna handlingar (2 kap. 1 § tryckfrihetsförordningen). Rätten att ta del av allmänna handlingar gäller i förhållande till enskilda och är inte tillämplig i förhållandet mellan myndigheter. Rätten är vid men kan begränsas med hänvisning till vissa hänsyn som räknas upp i 2 kap. 2 § tryckfrihetsförordningen. Godtagbara hänsyn kan till exempel vara rikets säkerhet eller dess förhållande till en annan stat eller en mellanfolklig organisation, intresset av att förebygga eller beivra brott, det allmännas ekonomiska intresse, skyddet för enskildas personliga eller ekonomiska förhållanden.

Begränsningar av rätten att ta del av allmänna handlingar följer främst av offentlighets- och sekretesslagen (2009:400) (OSL) som innehåller bestämmelser om sekretess för innehåll i allmänna handlingar. Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 § OSL).

Sekretess gäller både i förhållande till enskilda personer och andra myndigheter (8 kap. 1–2 §§ OSL). Syftet med sekretess mellan myndigheter är främst att värna den personliga integriteten hos en enskild vars uppgifter förekommer hos en myndighet.[1]

Sekretess kan även gälla inom en myndighet om det finns olika verksamhetsgrenar och dessa kan betraktas som självständiga i förhållande till varandra.[2]

Sekretess kan också gälla i förhållande till utländska myndigheter och mellanfolkliga organisationer (8 kap. 3 § OSL).

En sekretessbestämmelse är normalt uppbyggd med tre rekvisit; sekretessens föremål, räckvidd och styrka. Dessa rekvisit anger under vilka förutsättningar sekretess gäller för en viss uppgift.

Föremålet för sekretess är den uppgift som skyddas av sekretess. Vilka uppgifter som kan blir föremål för sekretess styrs av den nämnda uppräkningen i 2 kap. 2 § tryckfrihetsförordningen. Sekretessens *räckvidd* anger i vilken utsträckning uppgiften i bestämmelsen är belagd med sekretess. Räckvidden kan vara generell eller begränsad till en

[1] Prop. 1979/80:2 *med förslag till sekretesslag m.m.*, Del A s. 90.
[2] Se till exempel prop. 2008/09:150 *Offentlighets- och sekretesslag*, s. 359–360.

viss typ av ärenden, till en viss typ av verksamhet eller gälla vid en viss myndighet. Det tredje rekvisitet är sekretessens *styrka* som bestäms med ett s.k. skaderekvisit. Ett skaderekvisit kan vara antingen rakt eller omvänt. Ett rakt skaderekvisit innebär en presumtion för att uppgifterna är offentliga och att sekretess gäller först om det kan antas att viss skada uppstår om uppgiften lämnas ut. Vid ett omvänt skaderekvisit är utgångspunkten den motsatta, uppgifterna omfattas av sekretess om det inte står klart att uppgiften kan lämnas ut utan att viss skada uppstår. Sekretessens styrka kan i vissa fall bero på vilken grad av skada som krävs för att sekretess ska gälla, s.k. kvalificerat skaderekvisit. Sekretess kan även vara absolut, dvs. uppgiften omfattas av sekretess utan att någon skadeprövning görs när uppgiften begärs ut. Om en bestämmelse saknar skaderekvisit innebär det normalt att uppgifter omfattas av absolut sekretess.

Utöver de tre rekvisiten begränsas en sekretessbestämmelses tillämplighet vanligtvis även i tid. Sekretess för uppgift i allmänna handlingar begränsas som regel om det är fråga om personliga förhållanden med en sekretesstid om högst 70 år och om det är fråga om sekretess till skydd för enskilds ekonomiska förhållanden högst 20 år.

Om en uppgift omfattas av en sekretessbestämmelse får den inte lämnas ut utan lagstöd. Myndigheter har i många fall behov av att utbyta information, även sådan som omfattas av sekretess. För att möjliggöra ett effektivt informationsutbyte mellan myndigheter finns det i OSL en rad sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess. En sekretessbrytande bestämmelse innebär att en sekretessbelagd uppgift under vissa förutsättningar får lämnas ut. En sådan bestämmelse innehåller vanligen en intresseavvägning mellan myndigheternas eller enskildas behov av att ta del av uppgiften och de intressen den aktuella bestämmelsen avser att skydda.

9.2.2 Sekretessbestämmelser till skydd för enskilds intressen

Ett flertal bestämmelser i OSL gäller till skydd för enskilds personliga förhållanden (se avsnitt V OSL). Vad som kan utgöra personliga förhållanden är ett begrepp som omfattar allt från en persons namn till uppgifter om en persons hälsotillstånd. I 21 kap. 1 § OSL regleras ett minimiskydd för enskilds personliga förhållanden som gäller

inom hela den offentliga sektorn, oavsett i vilket sammanhang eller vid vilken myndighet uppgiften förekommer.

Utöver de generella bestämmelserna i 21 kap. OSL finns också andra särskilda sekretessbestämmelser i OSL till skydd för enskild eller skydd för uppgift inom en aktörs ansvarsområde eller verksamhet.

Av relevans för utredningens uppdrag kan även nämnas bestämmelserna i 35 kap. OSL som gäller till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott, m.m. Sekretess enligt 35 kap. 1 § gäller vid Polismyndigheten och Säkerhetspolisen för uppgift om enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men, och uppgiften förekommer i till exempel en förundersökning i brottmål, angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott, annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av bland annat Polismyndigheten och Säkerhetspolisen. Sekretessbestämmelsen hindrar inte att en uppgift om en enskild lämnas mellan Polismyndigheten och Säkerhetspolisen, om den mottagande myndigheten behöver uppgiften i sin brottsbekämpande verksamhet (35 kap. 10 a §).

Sekretessbestämmelser till skydd för uppgifter om enskilds personliga förhållanden som förekommer i annan verksamhet vid Polismyndigheten följer främst av 35 kap. 20 §–23 b § OSL. I bestämmelserna regleras bland annat sekretess för vissa uppgifter i ärenden enligt 21 kap. föräldrabalken, ärende om omhändertagande eller handräckning enligt lagstiftningen om psykiatrisk tvångsvård eller rättspsykiatrisk vård eller om vård av missbrukare utan samtycke inom socialtjänsten.

9.2.3 Sekretessbestämmelser till skydd för allmänna intressen

I OSL finns även sekretessbestämmelser som gäller till skydd för allmänna intressen, till exempel uppgifter om försvaret, det allmännas ekonomiska intressen eller internationella relationer. I Polismyndighetens arbete, och specifikt vid tillämpningen av TCO-förordningen, aktualiseras främst bestämmelserna i 18 kap. OSL om skydd för det allmänna intresset att förebygga och beivra brott.

Sekretessbestämmelserna i 18 kap. OSL skyddar uppgifter som förekommer i Polismyndighetens och Säkerhetspolisens brottsförebyggande och brottsbekämpande arbete. *Förundersökningssekretess* gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs (18 kap. 1 §). Att en uppgift hänför sig till sådan verksamhet innebär inte att myndigheten som förvarar uppgiften själv behöver bedriva sådan verksamhet. Sekretessen överförs när uppgiften lämnas vidare från Polismyndigheten eller Säkerhetspolisen till en annan myndighet.

18 kap. OSL innehåller även i 2 § en bestämmelse om sekretess för uppgift som hänför sig till *underrättelseverksamhet*. Sekretessen gäller bland annat i Polismyndighetens och Säkerhetspolisens verksamhet. Bestämmelsen innehåller ett omvänt skaderekvisit vilket innebär att en uppgift som regel omfattas av sekretess om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Uppgifter som hänför sig till Polismyndighetens eller Säkerhetspolisens brottsförebyggande och brottsbekämpande verksamhet kan också skyddas genom bestämmelserna om utrikes- respektive försvarssekretess (se 15 kap. 1 § och 2 § OSL) och genom andra bestämmelser i 35 kap. OSL.

9.2.4 Sekretessbrytande bestämmelser och undantag från sekretess

Trots att en uppgift är skyddad av sekretess finns det situationer när intresset av att lämna ut en uppgift väger tyngre än det intresse sekretessbestämmelsen avser att skydda. I 10 kapitlet OSL finns ett antal generella sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess som kan tillämpas när myndigheter har behov av att utbyta sekretesskyddad information. Även i andra avsnitt i OSL finns det sekretessbrytande bestämmelser.

Med stöd av 10 kap. 2 § OSL kan sekretesskyddade uppgifter lämnas ut om det är *nödvändigt* för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen om nödvändigt utlämnande ska tillämpas restriktivt och inte enbart av effektivitetsskäl.

Det är den utlämnande myndighetens intresse av att lämna ut uppgiften som är avgörande för om bestämmelsen är tillämplig, inte vilket intresse den mottagande myndigheten har av att få del av uppgifterna.[3]

Generalklausulen i 10 kap. 27 § OSL ger myndigheter ytterligare en möjlighet att lämna sekretessbelagda uppgifter till en annan myndighet. Det krävs dock att det är *uppenbart* att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda. Möjligheten gäller även mellan olika verksamhetsgrenar inom samma myndighet. Rekvisitet ”uppenbart” indikerar att det är endast i helt klara situationer som utlämning kan ske. Generalklausulen ska inte tillämpas så att sekretessbelagda uppgifter lämnas ut slentrianmässigt.[4] Ett utlämnande ska som regel föregås av en grundlig prövning av en myndighet som mottar en begäran om utlämnande. I förarbetena till den äldre sekretesslagen uttalades att möjligheten att tillämpa generalklausulen och utväxla sekretessbelagda uppgifter får utnyttjas mer sparsamt och med större försiktighet om informationen inte är sekretesskyddad hos den mottagande myndigheten. Det gäller särskilt i fråga om uppgifter som skyddas av sekretess av hänsyn till enskildas intressen.[5]

I generalklausulens sista stycke anmärks att ett utlämnande med stöd av bestämmelsen inte heller får ske om utlämnandet strider mot lag eller förordning. Det innebär i praktiken att sekretessbelagda uppgifter inte får lämnas ut om det strider mot till exempel dataskyddslagstiftningen (se vidare nedan).

I anslutning till terrorismrelaterad brottslighet kan här nämnas att om en socialtjänst får kännedom om terrorbrottslighet (till exempel brottet offentlig uppmaning 3 § i rekryteringslagen) eller om det på grund av särskilda omständigheter finns risk för att en enskild kan komma att begå sådan brottslighet, så hindrar inte sekretessen i 26 kap. 1 § OSL att socialtjänsten lämnar en uppgift därom till Polismyndigheten eller Säkerhetspolisen (se 10 kap. 18 b § och 22 a § OSL).[6]

En annan möjlighet för myndigheter att utbyta sekretesskyddade uppgifter är med stöd av en uttrycklig bestämmelse om *uppgiftsskyl-*

[3] Se prop. 1979/80:2 Del A s. 465 och Lenberg, Tansjö och Geijer, Offentlighets- och sekretesslagen (2021-11-23, version 24, JUNO), kommentaren till 10 kap. 2 §.
[4] Se JO 2014/15 s. 127 och JO 2017/18 s. 275 angående utlämnade av uppgifter med stöd av generalklausulen mellan Polismyndigheten och Kronofogdemyndigheten.
[5] Prop. 1979/80:2 Del A s. 77.
[6] Bestämmelserna föreslås få en annan lydelse i prop. 2021/22:133 *En samlad straffrättslig terrorismlagtiftning*, s. 42–43 och 222 f.

dighet. Sekretess hindrar då inte att uppgifterna lämnas ut till en annan myndighet (10 kap. 28 § OSL). För att en bestämmelse om uppgiftsskyldighet ska utgöra ett undantag från sekretess krävs att den är konkret och inte endast en generell uppmaning till samverkan mellan myndigheter.[7]

9.2.5 Överföring av sekretess

När Polismyndigheten eller en annan myndighet tar emot uppgifter från en myndighet överförs normalt inte sekretessen till den mottagande myndigheten. Om Polismyndigheten får en uppgift från Säkerhetspolisen eller någon annan myndighet gäller sekretess för uppgiften hos Polismyndigheten endast om sekretess följer av en primär sekretessbestämmelse som är tillämplig hos myndigheten eller av en bestämmelse om överföring av sekretess (7 kap. 2 § OSL).

En primär sekretessbestämmelse är en bestämmelse om sekretess som en myndighet ska tillämpa på grund av att bestämmelsen riktar sig direkt till myndigheten eller omfattar en viss verksamhetstyp eller en viss ärendetyp som hanteras hos myndigheten eller omfattar vissa uppgifter som finns hos myndigheten.

En bestämmelse om överföring av sekretess (en sekundär sekretessbestämmelse) innebär att en sekretessbestämmelse som är tillämplig på en uppgift hos en myndighet, ska tillämpas på uppgiften även av en myndighet som uppgiften lämnas till eller som har elektronisk tillgång till uppgiften hos den förstnämnda myndigheten (3 kap. 1 § OSL).

9.3 Samverkan mellan myndigheter

Myndigheter har en generell skyldighet att inom sitt verksamhetsområde samverka med andra myndigheter (8 § förvaltningslagen [2017:900]). Skyldigheten är inte obegränsad. Den tillfrågade myndigheten ska i första hand prioritera myndighetens egna huvuduppgifter och avgöra om det finns resurser tillgängliga för att bistå den myndighet som efterfrågar hjälp.

För Polismyndighetens och Säkerhetspolisens vidkommande följer en uttrycklig samverkansskyldighet mellan myndigheterna av 6 §

[7] Se till exempel lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet.

polislagen (1984:387) och ytterligare bestämmelser därom finns i 26–30 §§ förordningen (2014:1102) med instruktion för Polismyndigheten och 11–15 §§ förordningen (2014:1103) med instruktion för Säkerhetspolisen.

Hur informationsdelning och samverkan mellan myndigheterna i praktiken kan genomföras styrs av om berörda uppgifter skyddas av sekretess eller inte hos myndigheten som mottar en begäran om utlämnande.

Om förfrågan rör uppgifter som inte är sekretessbelagda har myndigheten en generell skyldighet att på begäran av en annan myndighet lämna uppgifter som den förfogar över, om det inte skulle hindra arbetets behöriga gång (6 kap. 5 § OSL). Skyldigheten att lämna ut uppgifter till en annan myndighet omfattar varje uppgift som myndigheten förfogar över och är inte begränsad till uppgifter i allmänna handlingar.[8] Innan en myndighet lämnar uppgifter till en annan myndighet måste myndigheten säkerställa att utlämnandet är förenligt med sekretesslagstiftningen men även med de begränsningar som följer av dataskyddslagstiftningen.

Om samverkan rör uppgifter som omfattas av sekretess hos den utlämnande myndigheten krävs det att det finns stöd för ett utlämnande i OSL. Vidare är utgångspunkten att sekretessen hos den utlämnande myndigheten inte överförs till den mottagande. Anledningen till att sekretessen inte överförs är att sekretesshänsynen ska beaktas i det enskilda fallet och vägas mot intresset av insyn i myndigheternas verksamhet. En sådan avvägning kan resultera i att en uppgift som skyddas av sekretess hos den utlämnade myndigheten blir offentlig hos den mottagande myndigheten.[9]

För två samverkande myndigheter som delar information kan en sekretessbelagd uppgift som lämnas till en annan myndighet omfattas av sekretess hos den mottagande myndigheten om det följer av en primär sekretessbestämmelse, som är tillämplig hos den mottagande myndigheten, eller om det följer av en bestämmelse om överföring av sekretess. Om inte någon av dessa förutsättningar är uppfyllda blir uppgiften offentlig hos den mottagande myndigheten.

[8] Prop. 1979/80:2 Del A s. 361.
[9] Prop. 1979/80:2 Del A s. 75–76.

9.4 Utredningens överväganden rörande sekretess och informationsutbyte

9.4.1 Sekretess hos Polismyndigheten

Utredningens förslag: Sekretess ska gälla hos Polismyndigheten för uppgift i ärenden enligt TCO-förordningen och kompletteringslagen till skydd för enskilds personliga eller ekonomiska förhållanden, om det kan antas att en enskild eller någon närstående till honom eller henne lider men om uppgiften röjs. Sekretess ska gälla i högst 70 år.

Rätten att meddela och offentliggöra uppgifter bör ha företräde framför den tystnadsplikt som följer av den föreslagna sekretessbestämmelsen.

Utredningens bedömning: Befintlig sekretessreglering utgör ett tillräckligt skydd för uppgifter som vid ett utlämnande skulle kunna skada eller motverka Polismyndighetens och Säkerhetspolisens brottsbekämpande eller brottsförebyggande verksamhet.

En ny sekretessbestämmelse behövs

De uppgifter som Polismyndigheten kommer att hantera i ett TCO-ärende kommer att vara av mycket skilda slag. Utredningen ser inte någon möjlighet att uttömmande ange exakt vilka uppgifter som kan förekomma i ett TCO-ärende. Uppgifterna kan komma att vara generella och övergripande uppgifter så som information om grupperingar, symboler eller uttryck. Ärenden kan också komma att innehålla texter, bilder eller videos som visar allvarlig brottslighet. De kan också komma att innehålla uppgifter om enskildas personliga intressen, till exempel uppgift om fysiska eller juridiska personer har kopplingar till en terroristgrupp eller uppgift om en enskilds eller grupps religiösa eller politiska övertygelse och aktiviteter. I andra fall kan ärenden som rör sanktioner innehålla uppgifter om en värdtjänstleverantörs ekonomiska förhållanden.

Uppgifterna som kommer att hanteras kan komma från en rad olika källor. Ett TCO-ärende kan till exempel inledas efter inkomna uppgifter från allmänheten, Säkerhetspolisen eller andra myndig-

heter. Under handläggningen kan Polismyndigheten begära in och hantera uppgifter från till exempel Säkerhetspolisen, CVE eller FOI.

Utgångspunkten är att allmänheten har en omfattande rätt till insyn i offentlig verksamhet. Insyn i TCO-ärenden kan uppfattas som särskilt viktig eftersom de kan beröra grundläggande frågor om yttrandefrihet. Utredningens uppfattning är därför att möjligheten till insyn bör vara långtgående i TCO-ärenden.

De uppgifter Polismyndigheten kommer att hantera i TCO-ärenden kan dock vara känsliga både med hänsyn till allmänna och enskilda intressen. Det bör därför finnas utrymme att skydda vissa uppgifter med sekretess. Utredningen överväger i det följande vilka uppgifter som kan behöva skyddas och om sådana uppgifter skyddas i tillräcklig utsträckning av befintlig sekretessreglering eller om det finns behov att föreslå kompletterande lagstiftning.

När Polismyndigheten får in uppgifter som initierar ett TCO-ärende är det myndighetens utgångspunkt att dessa även kommer att tas om hand inom den brottsbekämpande eller brottsförebyggande verksamheten.

Definitionen av terrorisminnehåll i TCO-förordningen är nära sammanbunden med den straffrättsliga terrorismlagstiftningen. Endast innehåll som är olagligt omfattas av förordningen. Det innebär att om Polismyndigheten får in innehåll som visar att någon typ av brott har begåtts eller planeras att begås kommer myndigheten även att vidta åtgärder inom ramen för den brottsbekämpande verksamheten. Uppgifterna kommer således att resultera både i straffrättslig och administrativ verksamhet. Genom det straffrättsliga ärendet kommer uppgifterna att skyddas av sekretess med stöd av 18 kap. 1 § eller 2 § OSL. Uppgifter som skyddas av sekretess med stöd av dessa bestämmelser i Polismyndighetens brottsförebyggande eller brottsbekämpande verksamhet kommer även att vara skyddade av sekretess när de samtidigt förekommer i ett TCO-ärende (jfr ”sekretess gäller för uppgift som hänför sig till”).

Uppgifter som Säkerhetspolisen lämnar till Polismyndigheten kommer främst att vara hänförliga till Säkerhetspolisens underrättelseverksamhet eller till brottsutredningar. Sådana uppgifter är skyddade av sekretess vid Säkerhetspolisen med stöd av 18 kap. 1–2 §§ OSL. Detsamma gäller när de hanteras av Polismyndigheten till exempel i ett TCO-ärende. Även när sådana uppgifter lämnas till Polismyndigheten skyddas de av sekretess.

Utredningens bedömning är att det allmännas intresse att skydda uppgifter som vid ett utlämnande skulle kunna skada eller motverka brottsbekämpande eller brottsförebyggande verksamheter har ett tillräckligt skydd genom befintlig reglering i OSL. Det saknas därför behov av att föreslå en särskild sekretessbestämmelse som gäller för sådana uppgifter hos Polismyndigheten i TCO-ärenden.

Möjligheten att skydda uppgifter om enskilds personliga och ekonomiska förhållanden i ett TCO-ärende är dock begränsad i befintlig sekretessreglering. En anledning till detta är att Polismyndighetens handläggning av TCO-ärenden inte är en del av myndighetens brottsbekämpande verksamhet. De sekretessbestämmelser som är tillämpliga i Polismyndighetens brottsbekämpande verksamhet till skydd för enskilds intressen kan som regel inte tillämpas på uppgifter i ett TCO-ärende (se 35 kap. 1 § OSL).

Den generella bestämmelsen om sekretess för enskilds intresse i 21 kap. 1 § OSL är begränsad till att skydda uppgifter som rör enskilds hälsa eller sexualliv. Detta skydd är inte tillräckligt med hänsyn till de uppgifter som kan komma att hanteras i ett TCO-ärende.

Ett utlämnande av uppgifter i ett TCO-ärende kan få negativa konsekvenser för enskilds personliga och ekonomiska förhållanden. De negativa konsekvenserna får vägas mot allmänhetens rätt till insyn. Vid en sådan avvägning skulle intresset av att skydda enskilda i vissa fall kunna väga tyngre än rätten till insyn. Utredningen föreslår därför en sekretessbestämmelse som skyddar uppgifter om enskilds personliga och ekonomiska förhållanden hos Polismyndigheten i ett TCO-ärende.

Bestämmelsens utformning

Utredningens bedömning är att en ny sekretessbestämmelse bör införas i OSL för att skydda uppgifter om enskilds personliga och ekonomiska förhållanden. När utredningen överväger hur en sådan bestämmelse bör utformas är utgångspunkten 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.

En sekretessbestämmelse ska vidare utformas så specifikt som möjligt när det gäller sekretessens föremål, dvs. vilka uppgifter som bestäm-

melsen avser att skydda. Polismyndighetens handläggning av ett TCO-ärende kan omfatta uppgifter av mycket varierande slag. Som nämnts tidigare är det svårt att på förhand ange vilka typer av uppgifter som kan förekomma i TCO-ärenden. En begränsning av sekretessens föremål till att gälla endast vissa typer av uppgifter kan innebära att andra uppgifter faller utanför bestämmelsens tillämpningsområde. Bestämmelsen bör därför utformas till skydd för uppgifter om enskilds personliga och ekonomiska förhållanden (2 kap. 2 § tryckfrihetsförordningen).

Sekretessbestämmelsens räckvidd ska preciseras så specifikt som möjligt, dvs. den ska ange inom vilken typ av ärenden eller verksamhet som bestämmelsen ska tillämpas. Utredningens bedömning är att sekretess ska gälla hos Polismyndigheten i ärenden som myndigheten handlägger med anledning av uppdraget som behörig myndighet enligt TCO-förordningen.

Skaderekvisitet ska utformas så att inte fler uppgifter hemlighålls än vad som är oundgängligen nödvändigt för att skydda det intresse som föranlett bestämmelsen. Vanligtvis utformas sekretessbestämmelser till skydd för uppgifter om enskilda i en verksamhet som avser myndighetsutövning med ett rakt skaderekvisit, dvs. med en presumtion att uppgifterna är offentliga. Utredningen ser ingen anledning att frångå vad som är brukligt och föreslår att sekretessbestämmelsen ska utformas med ett rakt skaderekvisit vilket innebär att det ska råda en presumtion för offentlighet i TCO-ärenden.

Slutligen bör sekretessbestämmelsen innehålla en yttersta begränsning i tid. När det gäller sekretess till skydd för enskilds personliga och ekonomiska förhållanden är sekretesstiden som regel högst 70 år. Utredningen ser ingen anledning att frångå denna tid.

Den sekretessbestämmelse utredningen nu föreslår bör placeras i anslutning till befintliga sekretessbestämmelser som rör annan verksamhet vid Polismyndigheten i 35 kap. OSL.

Om ett beslut i ett TCO-ärende överklagas till förvaltningsdomstol gäller den ovan föreslagna sekretessen även vid domstolen (43 kap. 1 § OSL).

Rätten att meddela och offentliggöra uppgifter

Sekretess innebär både handlingssekretess och tystnadsplikt (3 kap. 1 § OSL). Tystnadsplikten medför en begränsning av yttrandefriheten som regleras i regeringsformen och Europakonventionen.

Rätten att meddela och offentliggöra uppgifter, vanligen kallad meddelarfriheten, som följer av tryckfrihetsförordningen har normalt företräde framför tystnadsplikten (1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1–2 §§ yttrandefrihetsgrundlagen). Meddelarfriheten innebär att det i viss utsträckning är möjligt att straffritt lämna uppgifter som normalt är sekretessbelagda för publicering i tryckt skrift, radio eller tv.

Meddelarfriheten har dock inte företräde framför handlingssekretessen (7 kap. 3 § första stycket 2 och 5 § tryckfrihetsförordningen och 5 kap. 1 § första stycket och 3 § 2 yttrandefrihetsgrundlagen). Det sagda innebär att det kan vara tillåtet att muntligen lämna ut en sekretessbelagd uppgift till en journalist men inte tillåtet att lämna ut den allmänna handling vari den sekretessbelagda uppgiften framgår.

I vissa fall kan rätten att meddela och offentliggöra uppgifter vara helt inskränkt, tystnadsplikten i sekretessbestämmelsen har då företräde framför meddelarfriheten.

När utredningen nu föreslår en ny sekretessbestämmelse ska utredningen även överväga om den tystnadsplikt som följer av sekretessbestämmelsen bör inskränka rätten att meddela och offentliggöra uppgifter eller om denna rätt ska ha företräde framför tystnadsplikten.

Utgångspunkten är att meddelarfriheten endast ska begränsas i de fall där det är särskilt motiverat. Av förarbetena till den tidigare sekretesslagen uttalades att det finns större anledning att överväga undantag från meddelarfriheten när det är fråga om sekretessregler utan skaderekvisit och när det gäller bestämmelser med ett omvänt skaderekvisit än i andra fall.[10]

Den sekretessbestämmelse utredningen föreslår innehåller ett rakt skaderekvisit, vilket innebär en presumtion för offentlighet. Utformningen av bestämmelsen talar inte för att meddelarfriheten bör inskränkas. Det har inte heller framkommit några särskilda skäl som talar för att begränsa meddelarfriheten. Utredningen föreslår därmed inte någon begränsning av meddelarfriheten med anledning av den nya sekretessbestämmelsen.

[10] Prop. 1979/80:2 del A s. 111.

9.4.2 Uppgiftsskyldighet

Utredningens förslag: Säkerhetspolisen ska bistå den behöriga myndigheten i uppdraget som behörig myndighet enligt TCO-förordningen. En särskild bestämmelse om uppgiftsskyldighet bör föras in i kompletteringslagen.

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

Säkerhetspolisen ska ha rätt att på begäran ta del av de uppgifter hos den behöriga myndigheten som behövs för att bistå den behöriga myndigheten.

Uppgifter ska lämnas om inte särskilda skäl talar mot det.

Polismyndigheten ska utföra uppdraget som behörig myndighet utan att efterfråga eller ta emot instruktioner från någon annan aktör (artikel 13.2 TCO-förordningen). Det innebär att Polismyndigheten ska vara självständig och oberoende i sin myndighetsutövning. Det hindrar inte att Polismyndigheten kan behöva samverka med andra aktörer för att utbyta och samla in vissa uppgifter. Det kan till exempel handla om underlag som myndigheten anser sig behöva för att bedöma om visst innehåll ska anses vara terrorisminnehåll. De aktörer som kan vara aktuella att samverka med är främst myndigheter som har särskild kunskap om terrorism och terrorismrelaterade frågor. Här har, som nämnts tidigare, framför allt Säkerhetspolisen en viktig roll men även CVE och FOI.

Uppgifter som Polismyndigheten kan ha behov av kan vara av generell och övergripande karaktär. Sådana uppgifter omfattas normalt inte av sekretess vid myndigheten som förvarar uppgiften. Samverkan och utbyte av information kan då ske med stöd av de generella samverkansskyldigheterna mellan myndigheter som följer av lag (se 8 § förvaltningslagen, 26–30 §§ förordningen [2014:1102] med instruktion för Polismyndigheten, 11–15 §§ förordningen [2014:1103] med instruktion för Säkerhetspolisen och 6 kap. 5 § OSL), dock först efter beaktande av relevant dataskyddslagstiftning.

Andra uppgifter som Polismyndigheten kan ha behov av kan omfattas av sekretess vid den myndighet som förvarar uppgifterna. Utredningen har ovan pekat ut Säkerhetspolisen som en viktig myn-

dighet för Polismyndigheten att samverka med. Säkerhetspolisen har uppgett till utredningen att de uppgifter som kan vara aktuella att utbyta inom ramen för samverkan främst bör vara hänförliga till Säkerhetspolisens underrättelseverksamhet och därför är sådana att de omfattas av sekretess med stöd av 18 kap. 2 § och 35 kap. 1 § OSL. När det gäller uppgifter om en enskilds eller grupps kopplingar till terrorism anser Säkerhetspolisen att det främst är skyddet för enskild i 35 kap. 1 § OSL som kan utgöra ett hinder mot att utbyta relevanta uppgifter med Polismyndigheten i TCO-ärenden.[11]

Generalklausulen i 10 kap. 27 § OSL och bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § OSL ger vissa möjligheter för myndigheter att utbyta sekretesskyddade uppgifter. Bestämmelserna är avsedda att användas restriktivt och inte vid ett regelbundet uppgiftsutbyte. Bestämmelsen i 10 kap. 27 § OSL kan dessutom i många fall kräva svåra bedömningar av uppenbarhetsrekvisitet. Något som kan hindra ett effektivt informationsutbyte mellan myndigheterna.

Samverkan mellan Polismyndigheten och Säkerhetspolisen kan komma att bli regelbunden. Det är därför inte lämpligt att grunda ett regelbundet, och i vissa fall brådskande, informationsutbyte på de ovan nämnda sekretessbrytande bestämmelserna. För att underlätta samarbetet mellan Polismyndigheten och Säkerhetspolisen och säkerställa att det finns ett tydligt stöd för att lämna ut sekretesskyddade uppgifter bör en särskild bestämmelse införas som underlättar informationsutbytet mellan dessa myndigheter. En sådan bestämmelse bör säkerställa:

– att Säkerhetspolisen lämnar ut de uppgifter som Polismyndigheten kan behöva för att utföra uppdraget som behörig myndighet enligt TCO-förordningen, och

– att Säkerhetspolisen har rätt att ta del av de uppgifter hos Polismyndigheten som de behöver för att bistå Polismyndigheten i sitt uppdrag som behörig myndighet.

Det finns olika sätt att utforma en bestämmelse som uppfyller dessa krav. Utredningen har stannat för att det är lämpligast att föreslå en bestämmelse om uppgiftsskyldighet mellan Polismyndigheten och

[11] Liknande bedömning har gjorts i andra lagstiftningsärende, se till exempel betänkandena *Rätt mottagare – Granskning och integritet*, SOU 2021:99, s. 141 och *Informationsutbyte vid samverkan mot terrorism* SOU 2018:65 s. 210.

Säkerhetspolisen som utformas med stöd av 10 kap. 28 § OSL. En sådan uppgiftsskyldighet innebär att sekretess vid myndigheterna inte hindrar att en uppgift lämnas ut. För att bryta sekretessen måste uppgiftsskyldigheten framgå av lag eller annan författning.

Frågan är var en sådan bestämmelse bör placeras. Utredningen har övervägt tre alternativ. Ett alternativ är att placera uppgiftsskyldigheten i förordningen (2014:1103) med instruktion för Säkerhetspolisen.[12] Bestämmelsen skulle också kunna placeras i en speciallag om myndighetssamverkan[13] eller i den kompletteringslag som utredningen föreslår i detta betänkande. De befintliga speciallagar om myndighetssamverkan som utredningen känner till rör andra former av reglerad samverkan, främst i de berörda myndigheternas brottsbekämpande verksamhet. Som utredningen tidigare redovisat utgör Polismyndighetens handläggning av ärenden enligt TCO-förordningen administrativa ärenden och är inte en del av den brottsbekämpande verksamheten. Någon lämplig befintlig lag om samverkan finns därför inte. Utredningen bedömer att det är mest lämpligt att placera uppgiftsskyldigheten i lag, till skillnad mot en förordning, och i anslutning till övriga nationella bestämmelser som kompletterar TCO-förordningen. Bestämmelsen om uppgiftsskyldighet ska därför placeras i kompletteringslagen.

Det finns vissa situationer när den uppgiftsskyldighet som utredningen föreslår inte blir tillämplig. I OSL finns ett antal bestämmelser som främst rör sekretess för uppgifter som härrör från internationella avtal. I dessa bestämmelser framgår att en sekretessbrytande bestämmelse som meddelats med stöd av 10 kap. 28 § OSL får inte tillämpas i strid med aktuella sekretessbestämmelsen. Se till exempel 15 kap. 1 a §, 27 kap. 5 § och 34 kap. 4 § OSL.

Det kan också finnas uppgifter som omfattas av sekretess vid Säkerhetspolisen och Polismyndigheten som är särskilt känsliga. Utredningen föreslår därför att en uppgift inte ska lämnas ut om särskilda skäl talar mot det. Det är den utlämnande myndigheten som prövar om det finns särskilda skäl mot att lämna ut en uppgift.

Utredningen bedömer att samverkan och informationsutbyte mellan Polismyndigheten och andra myndigheter, till exempel FOI och CVE, kan komma att ske i väsentligt mindre utsträckning. Ett utläm-

[12] Se förordningen (2014:1103) med instruktion för Säkerhetspolisen och den uppgiftsskyldigheten som föreslås i *Anpassning av svensk rätt till EU:s nya system för reseuppgifter och resetillstånd*, Ds 2021:19, s. 27.
[13] Se lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet.

nande av sekretesskyddade uppgifter bör i dessa situationer kunna ske med stöd av generalklausulen i 10 kap. 27 § OSL.

9.4.3 Informationsutbyte mellan medlemsstaternas behöriga myndigheter

Utredningens bedömning: Den behöriga myndigheten kan utbyta information inom ramen för TCO-förordningen med stöd av artikel 14 i TCO-förordningen.

En uppgift som skyddas av sekretess hos den behöriga myndigheten får i två situationer lämnas ut till en utländsk myndighet eller mellanfolklig organisation. Utlämnandet ska ske i enlighet med en föreskrift i lag eller förordning eller om uppgiften i motsvarande fall skulle få lämnas ut till svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller mellanfolkliga organisationen (8 kap. 3 § OSL). En föreskrift i en EU-förordning är att jämställa med en föreskrift i lag eller förordning.[14]

I artikel 14 TCO-förordningen framgår att 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. Ett utbyte av information mellan Polismyndigheten och andra medlemsstaters behöriga myndigheter kan därför ske med direkt stöd av artikel 14.

9.4.4 Förhållandet till dataskyddslagstiftningen[15]

Utredningens bedömning: Den behöriga myndigheten kommer att behandla personuppgifter vid handläggning av TCO-ärenden. En del av behandlingen kommer att avse känsliga personuppgifter.

[14] Prop. 2018/19:38 *Kompletterande bestämmelser till EU:s förordning om transparens i transaktioner för värdepappersfinansiering och om återanvändning*, s. 88.
[15] Här avses i första hand Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter

Även samverkan mellan den behöriga myndigheten och andra myndigheter, främst Säkerhetspolisen, kommer att innebära personuppgiftsbehandling.

Det finns rättslig grund för behandling av personuppgifter inom ramen för ett TCO-ärende vid Polismyndigheten och Säkerhetspolisen.

Tillämpningen av TCO-förordningen och kompletteringslagen kan innebära intrång i den personliga integriteten. Vikten av att genomföra de åtgärder som följer av TCO-förordningen väger dock tyngre än skyddet för den personliga integriteten. Personuppgiftsbehandlingen utgör därför ett godtagbart integritetsintrång och får anses proportionerlig.

Personuppgiftsbehandling i samband med tillämpningen av TCO-förordningen och kompletteringslagen anses förenlig med befintlig dataskyddslagstiftning.

Allmänna utgångspunkter

Den behöriga myndighetens handläggning av TCO-ärenden och samverkan med andra myndigheter aktualiserar, utöver sekretessfrågor, även frågor om dataskydd eftersom uppdraget innebär behandling av personuppgifter[16]. I detta avsnitt analyserar utredningen om den utökade personuppgiftsbehandlingen är förenlig med befintlig dataskyddslagstiftning eller om det behövs ytterligare lagstiftning.

För att få behandla personuppgifter krävs att dataskyddslagstiftningen tillåter det. Vid bedömningen nedan utgår utredningen från att Polismyndigheten utses till behörig myndighet. Inledningsvis bedömer utredningen att brottsdatalagen inte är tillämplig i ett TCO-ärende eftersom behandling av personuppgifter inte kommer att ske i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller

och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordning), lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen), Brottsdatalag (2018:1177) och lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.

[16] *Personuppgifter* definieras i artikel 4.1. dataskyddsförordningen som personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

verkställa straffrättsliga påföljder (1 kap. 2 § brottsdatalagen). Även om effekterna av TCO-förordningen kan bli positiva för det brottsförebyggande och brottsbeivrande arbetet sker personuppgiftsbehandling i ett TCO-ärende främst i andra syften. De generella bestämmelserna i dataskyddsförordningen och dataskyddslagen är därför tillämpliga.

Personuppgiftsbehandling kräver att en rad grundläggande principer i artikel 5 dataskyddsförordningen är uppfyllda, till exempel att personuppgifterna behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (artikel 5.1.a) och att de endast ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (artikel 5.1.b). Den omständigheten att personuppgifter inte senare får behandlas på ett sätt som är oförenligt med ändamålen är ett uttryck för finalitetsprincipen. Principen innebär att om en tilltänkt behandling av redan insamlade personuppgifter inte omfattas av de ursprungliga ändamålen måste det göras en bedömning av om ändamålet med den senare behandlingen är förenlig med de ursprungliga ändamålen eller inte.[17]

För att personuppgiftsbehandling ska vara förenlig med dataskyddsförordningen måste det även finnas en rättslig grund i artikel 6 dataskyddsförordningen för behandlingen. Rättsliga grunder för behandling kan till exempel vara att den registrerade lämnat sitt samtycke (artikel 6.1 a), att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c) eller att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller utgör ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e).

Bestämmelserna i dataskyddsförordningen utvecklas ytterligare i dataskyddslagen. Där framgår att personuppgifter får behandlas med stöd av artikel 6.1 c om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning (2 kap. 1 § dataskyddslagen). I 2 kap. 2 § dataskyddslagen förtydligas vidare att personuppgifter får behandlas med stöd av artikel 6.1 e i data-

[17] Se vidare Högsta förvaltningsdomstolens avgörande i HFD 2021 ref. 10 där frågan var om en bestämmelse om uppgiftsskyldighet var förenlig med bland annat finalitetsprincipen i dataskyddsförordningen.

skyddsförordningen, om behandlingen är nödvändig för att utföra 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, eller som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Personuppgiftsbehandling hos Polismyndigheten

Den behöriga myndigheten – Polismyndigheten – kommer att ha en rättsligt reglerad förpliktelse att utföra de uppgifter som följer av TCO-förordningen och kompletteringslagen (2 kap. 1 § dataskyddslagen). För att fullgöra förpliktelserna i TCO-förordningen är personuppgiftsbehandling nödvändig hos Polismyndigheten. Uppdraget som behörig myndighet är en uppgift av allmänt intresse som kommer att fastställas i svensk rätt. Det finns därför rättslig grund för den behöriga myndigheten att behandla personuppgifter.

De uppgifter som Polismyndigheten sannolikt kommer att behandla är bland annat information om misstänkt terrorisminnehåll som lämnas in från allmänheten, andra aktörer eller myndigheter. Det kan också förekomma uppgifter om brott eller brottsmisstankar och om enskilda individer som kan kopplas till terroristgrupper. Även uppgifter om berörda värdtjänstleverantörer och innehållsleverantörer kan förekomma.

Det kan inte uteslutas att Polismyndigheten även kommer att behandla personuppgifter som till exempel avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse (artikel 9.1 dataskyddsförordningen). Utgångspunkten är att behandling av sådana personuppgifter endast får ske om förutsättningarna i artikel 9.2 är uppfyllda till exempel om den registrerade lämnat sitt samtycke eller om det är nödvändigt av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt. Behandlingen ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen (artikel 9.2).

Polismyndighetens uppdrag som behörig myndighet enligt TCO-förordningen är en uppgift av allmänt intresse. Det finns därmed för-

utsättningar för den behöriga myndigheten att behandla känsliga personuppgifter.

En ökad hantering av personuppgifter innebär risker för skyddet av den personliga integriteten. Vikten av att genomföra de åtgärder som följer av TCO-förordningen väger dock tyngre än skyddet för den personliga integriteten. TCO-förordningen och de förslag som utredningen lämnar kommer att leda till ökad hantering av personuppgifter men dessa anser utredningen är proportionerliga och får godtas.

Personuppgiftsbehandling hos Säkerhetspolisen

Samverkan mellan Säkerhetspolisen och Polismyndigheten kommer även att föranleda personuppgiftsbehandling hos Säkerhetspolisen. Säkerhetspolisens behandling av personuppgifter regleras huvudsakligen i lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Vid personuppgiftsbehandling i administrativa ärenden tillämpas dock dataskyddsförordningen och dataskyddslagen.

Personuppgifter, som behandlas för någon av de rättsliga grunder som anges i 2 kap. 1 § nämnda lag, får behandlas vid Säkerhetspolisen om det är nödvändigt för att tillhandahålla information som behövs i en myndighets verksamhet om Säkerhetspolisen enligt lag eller förordning ska bistå myndigheten med en viss uppgift (2 kap. 4 § första stycket fjärde punkten).

Personuppgifter får även behandlas hos Säkerhetspolisen om det är nödvändigt för att tillhandahålla information till riksdagen eller regeringen och, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra (2 kap. 4 § andra stycket). Säkerhetspolisens skyldighet att bistå Polismyndigheten kommer att regleras genom en uppgiftsskyldighet i kompletteringslagen. Utredningens bedömning är mot den bakgrunden att det finns rättslig grund för behandling av personuppgifter hos Säkerhetspolisen inom ramen för samverkan med Polismyndigheten i TCO-ärenden.

10 Övriga ändringar i svensk rätt

10.1 Inledning

En del av utredningens uppdrag är att överväga om det finns behov av ändringar i svensk rätt med anledning av TCO-förordningen. I detta kapitel analyserar därför utredningen TCO-förordningens förhållande till 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 överväger om det finns behov av att föreslå författningsändringar.

10.2 Lagen om ansvar för elektroniska anslagstavlor (BBS-lagen)

10.2.1 Allmänt om BBS-lagen

BBS-lagen reglerar en skyldighet för tillhandahållare av elektroniska anslagstavlor att – under vissa förutsättningar – ta bort meddelanden från tjänsten. Lagen benämns ofta BBS-lagen vilket är en förkortning av den engelska beteckningen på elektronisk anslagstavla, Bulletin Board System. En elektronisk anslagstavla kan beskrivas som en interaktiv tjänst för elektronisk förmedling av meddelanden där användaren kan publicera information, till exempel interaktiva webbsidor med diskussionsforum, kommentatorsfält eller chattfunktion.[1] Ett meddelande kan bestå av text, bild, ljud eller information i övrigt (1 § andra stycket).

Lagen är inte tillämplig på tillhandahållande av endast nät eller andra förbindelser för överföring av meddelanden eller av andra anord-

[1] Edmar, M. *Internetpublicering och sociala medier, En juridisk vägledning* (2021, version 7, JUNO), s. 219–220.

ningar som krävs för att kunna ta i anspråk ett nät eller annan förbindelse, förmedling av meddelanden inom en myndighet eller mellan myndigheter eller inom ett företag eller en koncern, tjänster som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller meddelanden som är avsedda bara för en viss mottagare eller en bestämd krets av mottagare (e-post) (2 §).

En tillhandahållare i BBS-lagen är den som kan bestämma över tjänstens användning, inklusive de tekniska och administrativa rutinerna.[2]

Den som tillhandahåller en elektronisk anslagstavla ska, för att fullgöra sin skyldighet i 5 §, ha sådan uppsikt över tjänsten som skäligen kan krävas med hänsyn till omfattningen och inriktningen av verksamheten (4 §). Uppsikten innebär inte att tillhandahållaren aktivt ska kontrollera varje enskilt meddelande men att det görs någon form av återkommande kontroll. Ett sätt att uppfylla uppsiktsplikten, som föreslås i förarbetena, kan vara att inrätta en ”klagomur” dit användarna har möjlighet att anmäla olagligt innehåll som påträffas på tjänsten.[3]

I 5 § framgår, såvitt är av relevans här, att 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 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,

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

g) offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.[4]

[2] Prop. 1997/98:15 *Ansvar för elektroniska anslagstavlor*, s. 10.
[3] Prop. 1997/98:15 s. 15.
[4] Utredningen återkommer nedan under avsnitt 10.2.2 till de ändringar av BBS-lagen och 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet som föreslås i prop. 2021/22:133 *En samlad straffrättslig terrorismlagstiftning*.

Lagstiftaren har kopplat kravet på att ta bort ett meddelande till innehållet i meddelandet. Eftersom elektroniska anslagstavlor ofta tillhandahålls av personer som inte yrkesmässigt tillhandahåller tjänster ansåg lagstiftaren att det inte var rimligt att begära att tillhandahållaren skulle kunna ta ställning till svåra juridiska gränsdragningsproblem.[5] Det infördes därför ett uppenbarhetsrekvisit i lagen, om innehållet *uppenbart* faller in under de i bestämmelsen uppräknade brotten ska meddelandet tas bort eller dess spridning på annat sätt förhindras.

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. I ringa fall ska det inte dömas till ansvar (7 §).

BBS-lagen har endast tillämpats i begränsad omfattning. I rättsfallet NJA 2007 s. 805 I prövade Högsta domstolen BBS-lagens tillämpningsområde och uppenbarhetsrekvisitet. I målet hade en person som administrerat en elektronisk anslagstavla åtalats för att ha underlåtit att ta bort meddelanden som åklagaren gjorde gällande uppenbart utgjorde hets mot folkgrupp. Högsta domstolen ansåg att meddelandena överskred gränsen för vad som objektivt sett är att bedöma som hets mot folkgrupp. Mot bakgrund av bland annat skyddet för yttrande- och religionsfrihet i Europakonventionen, ansåg domstolen att innehållet i meddelandena inte *uppenbart* utgjorde hets mot folkgrupp varför åtalet ogillades.

Ett rättsfall som meddelats i mer närtid är Svea hovrätts dom från den 4 december 2020 (mål B 8432-19). I det målet dömdes en administratör av en grupp på Facebook för brott mot BBS-lagen för att inte ha tagit bort eller förhindrat vidare spridning av inlägg vars innehåll uppenbart utgjorde hets mot folkgrupp.

10.2.2 Särskilt om offentlig uppmaning

Ett av de brott som räknas upp i 5 § BBS-lagen är offentlig uppmaning. Brottet offentlig uppmaning infördes i svensk rätt genom 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen). Kriminaliseringen var en del av Sveriges

[5] Prop. 1997/98:15 s. 17.

genomförande av Europarådets konvention om förebyggande av terrorism (ETS 196) och 2008 års rambeslut[6].

Genom bestämmelsen i rekryteringslagen är det straffbart att i ett meddelande till allmänheten uppmana eller annars söka förleda till särskilt allvarlig brottslighet eller till samröre med en terroristorganisation enligt 2 b § rekryteringslagen. Straffskalan för brottet är fängelse i högst två år. Med särskilt allvarlig brottslighet i 2 § rekryteringslagen avses bland annat terroristbrott enligt lagen (2003:148) om straff för terroristbrott. I förarbetena till rekryteringslagen uttryckte lagstiftaren att brottet offentlig uppmaning redan motsvaras i svensk rätt av uppvigling i 16 kap. 5 § brottsbalken men att det ändå fanns skäl att särreglera offentlig uppmaning genom att införa det i rekryteringslagen.[7]

Sverige har därefter tillträtt tilläggsprotokollet[8] till Europarådets konvention om förebyggande av terrorism och EU har antagit terrorismdirektivet[9]. Terrorismdirektivet förtydligar i artikel 5 att offentlig uppmaning omfattar spridande, eller tillgängliggörande för allmänheten på annat sätt, oavsett metod, såväl på som utanför internet, av meddelanden. Åtgärder mot innehåll på internet som utgör offentlig uppmaning behandlas särskilt i artikel 21 terrorismdirektivet. Där framgår att medlemsstaterna ska vidta nödvändiga åtgärder för att säkerställa att internetinnehåll som finns på servrar på deras territorium och som utgör en offentlig uppmaning till terroristbrott utan dröjsmål ska avlägsnas. Medlemsstaterna ska också sträva efter att avlägsna innehåll på servrar utanför deras territorium. I artikel 21 framgår vidare att när det inte är genomförbart att avlägsna innehållet vid källan kan medlemsstaterna vidta åtgärder för att blockera åtkomsten till innehåll för internetanvändarna inom sitt territorium. Åtgärder för avlägsnande och blockering måste inrättas i enlighet med transparenta förfaranden och tillhandahålla adekvata skyddsmekanismer,

[6] Rådets rambeslut 2008/919/RIF av den 28 november 2008 om ändring av rambeslut 2002/475/RIF om bekämpande av terrorism.
[7] Uppvigling 16 kap. 5 § första stycket brottsbalken ”Den som muntligen inför menighet eller folksamling, i skrift som sprides eller utlämnas för spridning eller i annat meddelande till allmänheten uppmanar eller eljest söker förleda till brottslig gärning, svikande av medborgerlig skyldighet eller ohörsamhet mot myndighet, dömes för uppvigling till böter eller fängelse i högst sex månader.” Se prop. 2009/10:78 *Straffrättsliga åtgärder till förebyggande av terrorism* s. 29 f. och s. 44.
[8] Tilläggsprotokoll till Europarådets konvention om förebyggande av terrorism (som antogs av ministerkommittén vid dess 125:e session den 19 maj 2015).
[9] Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF.

särskilt för att säkerställa att åtgärderna begränsas till vad som är nödvändigt och proportionellt. Användarna ska informeras om orsaken till åtgärderna. Skyddsmekanismer i samband med avlägsnande eller blockering ska omfatta en möjlighet till rättslig prövning.

Vid implementeringen av terrorismdirektivet bedömde lagstiftaren att Sverige uppfyllde direktivets krav i artikel 21.1 genom befintlig reglering i brottsbalken, rättegångsbalken, e-handelslagen och bestämmelserna i BBS-lagen där, som framgått ovan, uppvigling är ett av de uppräknade brotten i 5 §. I förtydligande syfte utvidgades dock uppräkningen i 5 § BBS-lagen till att även omfatta offentlig uppmaning till särskilt allvarlig brottslighet enligt 3 § rekryteringslagen. Eftersom straffbestämmelsen i 5 § BBS-lagen är subsidiärt tillämplig i förhållande till bland annat brottsbalken ändrades även subsidiaritetsbestämmelsen i 7 § så att straff enligt BBS-lagen inte kan utdömas om det för gärningen kan dömas till ansvar enligt rekryteringslagen.[10]

Bestämmelsen i terrorismdirektivet om en möjlighet att blockera innehåll föranledde överväganden i betänkandet *Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism* (SOU 2017:72). En skyldighet att blockera visst innehåll på internet hade då tidigare införts genom barndirektivet[11]. Vid implementeringen av barndirektivet ansågs Sverige uppfylla kravet på blockering av barnpornografiskt innehåll på internet genom ett frivilligt samarbete mellan Polismyndigheten och ett antal Internet Service Providers (ISPs), även kallat Blockeringsprojektet.[12] Vid implementeringen av artikel 21 terrorismdirektivet bedömde utredningen att det inte var lämpligt att utvidga det befintliga blockeringssamarbetet till att även omfatta innehåll på internet som utgör offentlig uppmaning. Utredningen kom fram till att bestämmelsen om blockering i terrorismdirektivet är fakultativ och, mot bakgrund av att Sverige uppfyller kraven i artikel 21.1, inte av sådan karaktär att den fordrar lagstiftning eller andra åtgärder.[13] Någon särskild bestämmelse om blockering kom inte att genomföras i svensk rätt med anledning av artikel 21.2 terrorismdirektivet.

[10] Prop. 2017/18:174 *En mer heltäckande terrorismlagstiftning*, s. 85 f.
[11] Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF.
[12] Se beskrivningen av projektet i SOU 2017:72 s. 270.
[13] SOU 2017:72 s. 271.

Den särskilda regleringen av offentlig uppmaning i rekryteringslagen bibehölls i samband med implementeringen av tilläggsprotokollet och terrorismdirektivet med argumenten att bestämmelsen fyller en viktig funktion genom att betona det särskilda allvaret i den brottslighet som uppmaningarna avser. Därtill är straffskalan i BBS-lagen strängare än bestämmelsen om uppvigling i brottsbalken. [14]

Regeringen föreslår i propositionen 2021/22:133 *En samlad straffrättslig terrorismlagstiftning* en ny terroristbrottslag för att skapa en mer ändamålsenlig, effektiv och överskådlig reglering i svensk rätt. Terroristbrottslagen kommer att, om den antas, ersätta bland annat rekryteringslagen och reglera straffansvar för terroristbrott, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet och resa för terrorism eller särskilt allvarlig brottslighet. Definitionen av terroristbrott föreslås ändras så att alla svenska uppsåtliga brott och försök till brott ska kunna utgöra terroristbrott, förutsatt att de allvarligt kan skada ett land eller en mellanstatlig organisation och begås med terrorismsyfte.

Beträffande straffansvaret för offentlig uppmaning föreslår regeringen att en bestämmelse om straffansvar för offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet förs in i 7 § terroristbrottslagen med följande lydelse.

> För *offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet* döms den som i ett meddelande till allmänheten uppmanar eller på annat sätt söker förleda till terroristbrott, särskilt allvarlig brottslighet eller brott som avses i 5 eller 6 § eller någon av 8–10 §§.
>
> Straffet är fängelse i högst tre år.
>
> Om brottet är grovt, döms till fängelse i lägst ett och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen
>
> 1. har avsett brottslighet som innefattar fara för flera människoliv eller för egendom av särskild betydelse,
>
> 2. har ingått som ett led i en verksamhet som har bedrivits i större omfattning,

[14] Prop. 2017/18:174 s. 75–76.

eller

3. på annat sätt har varit av särskilt farlig art.
Ringa fall utgör inte brott.

Den föreslagna lydelsen innebär att straffansvaret för offentlig uppmaning i framtiden även kommer att omfatta den som i ett meddelande till allmänheten uppmanar eller på annat sätt söker förleda till rekrytering till terrorism eller särskilt allvarlig brottslighet samt utbildning eller resa för terrorism eller särskilt allvarlig brottslighet.[15] För BBS-lagens vidkommande innebär den nya terroristbrottslagen vissa följdändringar. Regeringen föreslår i propositionen att 5 § och 7 § BBS-lagen i stället för rekryteringslagen ska hänvisa till 7 § terroristbrottslagen respektive terroristbrottslagen.[16]

10.2.3 Förhållandet till TCO-förordningen

Utredningens förslag: BBS-lagen ska inte vara tillämplig på meddelanden som omfattas av TCO-förordningen. En ny punkt i 2 § BBS-lagen bör införas där det framgår att BBS-lagen inte är tillämplig på meddelanden som omfattas av TCO-förordningen.

I 5 § BBS-lagen bör brottet offentlig uppmaning tas bort. Meddelanden som innehåller offentlig uppmaning kan komma att i stället bli föremål för åtgärder med stöd av TCO-förordningen och kompletteringslagen.

Till följd av utredningens förslag bör även hänvisningen i 7 § till lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet tas bort.

Både BBS-lagen och TCO-förordningen är tillämpliga på innehåll på internet som utgör offentlig uppmaning. BBS-lagen genom bland annat brottet offentlig uppmaning i 5 § och TCO-förordningen genom definitionen av terrorisminnehåll i artikel 2.7.

TCO-förordningen omfattar terrorisminnehåll som sprids på värdtjänster och BBS-lagen meddelanden som sprids på en elektronisk anslagstavla. Med utgångspunkt i TCO-förordningens defini-

[15] Prop. 2021/22:133 s. 106 f.
[16] Prop. 2021/22:133 s. 23–24 och 166.

tion av begreppet värdtjänst skulle dock en elektronisk anslagstavla kunna omfattas av förordningen. BBS-lagens och TCO-förordningens tillämpningsområde sammanfaller således i viss mån.

Till skillnad från TCO-förordningen kan dock BBS-lagen tillämpas även på privata, icke kommersiella tillhandahållare. Lagen har ur den aspekten ett vidare tillämpningsområde än TCO-förordningen. Ett meddelande som en privatperson, utan kommersiella intressen, publicerar på en elektronisk anslagstavla kan omfattas av skyldigheterna i BBS-lagen men inte av definitionen av begreppet värdtjänstleverantör och skyldigheterna i TCO-förordningen.

TCO-förordningen har företräde framför nationell rätt. Eftersom innehåll som omfattas av TCO-förordningen i vissa fall kan utgöra något av de uppräknade brotten i 5 § BBS-lagen, så som uppvigling eller olaga våldsskildring, kan BBS-lagen och TCO-förordningen komma att träffa samma innehåll. För att säkerställa att BBS-lagen inte kommer i konflikt med TCO-förordningen föreslår utredningen tre ändringar i BBS-lagen. Den första är ett tillägg i 2 § BBS-lagen som tydliggör att BBS-lagen inte är tillämplig på meddelanden som omfattas av TCO-förordningen. Den andra innebär att brottet offentlig uppmaning tas bort från uppräkningen i 5 § BBS-lagen. Meddelanden som innehåller offentlig uppmaning enligt 3 § rekryteringslagen kan i stället komma att bli föremål för åtgärder med stöd av TCO-förordningen och kompletteringslagen. Utredningens föreslagna ändringar innebär för det tredje att BBS-lagen inte längre ska tillämpas på meddelanden som omfattas av rekryteringslagen. Hänvisningen till den lagen bör därför tas bort från 7 §.

Om den nya terroristbrottslagen och de följdändringar som regeringen föreslår i prop. 2021/22:133 antas innebär utredningens bedömning ovan i stället att hänvisningen till offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet i 7 § terroristbrottslagen bör tas bort från 5 § BBS-lagen och att hänvisningen till terroristbrottslagen i 7 § BBS-lagen bör tas bort.

Offentlig uppmaning infördes i 5 § BBS-lagen som ett förtydligande av svensk lagstiftning i samband med implementeringen av terrorismdirektivet (se ovan). Det är utredningens uppfattning att Sverige även efter de föreslagna ändringarna kommer att uppfylla sina åtaganden enligt art. 21 terrorismdirektivet. Innehåll som i dag kan avlägsnas med stöd av BBS-lagen kommer sannolikt i stor utsträckning att i framtiden avlägsnas eller göras oåtkomligt med stöd av

TCO-förordningen. I ljuset av BBS-lagens historiskt sett begränsade tillämpning är det utredningens uppfattning att TCO-förordningen kan komma att utgöra ett mer kraftfullt verktyg mot terrorisminnehåll som sprids på internet och resultera i att innehåll i större utsträckning blir föremål för rättsliga eller frivilliga åtgärder när TCO-förordningen börjar tillämpas.

En effekt av utredningens förslag är dock att en tillhandahållare av en elektronisk anslagstavla, som inte är värdtjänstleverantör i TCO-förordningens mening, inte kommer att åläggas några skyldigheter i TCO-förordningen eller BBS-lagen för terrorisminnehåll som publiceras på tjänsten. Effekten kan framstå som mindre lämplig men utredningen har ändå stannat för att det är lämpligast att knyta det föreslagna undantaget i 2 § till det specifika meddelandet. Mot bakgrund av att fler rättsakter på EU-nivå i framtiden med all säkerhet kommer att reglera värdtjänstleverantörers ansvar för olagligt innehåll på internet lär ytterligare överväganden av BBS-lagens tillämpningsområde bli nödvändiga.

10.3 E-handelslagen

10.3.1 Allmänt om e-handelslagen

E-handelsdirektivet[17] har implementerats i svensk rätt huvudsakligen genom e-handelslagen. E-handelslagen reglerar i 16–19 §§ tjänsteleverantörers ansvarsfrihet i vissa fall för lagring eller överföring av innehåll. Bestämmelserna har vissa beröringspunkter med TCO-förordningen varför utredningen i detta avsnitt överväger om det finns behov av kompletterande författning för att genomföra TCO-förordningen i Sverige.

En tjänsteleverantör är enligt e-handelslagen en fysisk eller juridisk person som tillhandahåller någon av informationssamhällets tjänster (2 §). Informationssamhällets tjänster är tjänster som normalt utförs mot ersättning och som tillhandahålls på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare (2 §).

Utgångspunkten i e-handelslagen är att en tjänsteleverantör är fri från ansvar för den information som en tjänstemottagare lämnar på

[17] 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”).

tjänsten. Ansvarsfriheten gäller under förutsättning att leverantören inte känner till att den olagliga informationen eller verksamheten förekommer och, när det gäller skyldigheten att ersätta skada, inte är medveten om fakta eller omständigheter som gör det uppenbart att den olagliga informationen eller verksamheten förekommer, eller så snart leverantören får sådan kännedom eller medvetenhet utan dröjsmål förhindrar vidare spridning av informationen (18 §).

I förarbetena till e-handelslagen beskrivs syftet med ansvarsfriheten som ett sätt att säkerställa att värdtjänstleverantörer inte drabbas av ett orimligt stort ansvar. Lagstiftaren ansåg att ett alltför stort ansvar kunde hämma utvecklingen av informationssamhällets tjänster och hindra den inre marknaden.[18]

Ansvarsfriheten i e-handelslagen innebär att en tjänsteleverantör som överför eller lagrar information för annan får dömas till ansvar för brott som avser innehållet i informationen endast om brottet har begåtts uppsåtligen (19 §). Eftersom en värdtjänstleverantör sällan har vetskap om innehållet i den information som överförs eller lagras via leverantören är utrymmet att lagföra en värdtjänstleverantör i praktiken begränsat.[19]

E-handelsdirektivet innehåller även ett förbud mot att ställa krav på tjänsteleverantörer att övervaka den information de överför eller lagrar för annans räkning. Värdtjänstleverantörerna får enligt direktivet inte åläggas någon allmän skyldighet att aktivt efterforska fakta eller omständigheter som kan tyda på olaglig verksamhet. E-handelsdirektivet utgör enligt ingresspunkten 48 inget hinder mot att medlemsstater kräver att värdtjänstleverantörer visar ”den omsorg som skäligen kan förväntas av dem och vilken preciseras i nationell rätt, för att upptäcka och förhindra vissa slags olaglig verksamhet”. I förarbetena till e-handelslagen tolkades denna formulering i direktivet som att det är tillåtet för medlemsstaterna att kräva av värdtjänstleverantörer att ha viss uppsikt över sin tjänst, om det kan anses skäligt för att förhindra vissa typer av olaglig verksamhet. I den här kontexten har BBS-lagens bestämmelse om uppsikt inte ansetts strida mot övervakningsförbudet i e-handelsdirektivet.[20]

Ansvarsfrihetsreglerna hindrar inte domstolar och myndigheter från att med stöd av nationell rätt kräva att en tjänsteleverantör upp-

[18] Prop. 2001/02:150 *Lag om elektronisk handel och andra informationssamhällets tjänster, m.m.*, s. 87.
[19] Prop. 2001/02:150 s. 90.
[20] Prop. 2001/02:150 s. 100.

hör med eller förhindrar en överträdelse. E-handelsdirektivet ger medlemsstaterna en möjlighet att inrätta särskilda förfaranden för att avlägsna eller på annat sätt göra information oåtkomlig på internet. I förarbetena till e-handelslagen beskrivs dessa ”notice and take down”-regler, som en skyldighet för värdtjänstleverantörer att ta emot anmälningar om olagligt innehåll, avlägsna eller göra materialet otillgängligt och en rätt för en innehållsleverantör att överklaga sådana beslut till domstol. När direktivet implementerades i svensk rätt ansåg dock lagstiftaren att det inte fanns tillräckliga förutsättningar för att inrätta ett sådant ”notice and take down”-förfarande i Sverige.[21]

10.3.2 Förslaget till Digital Services Act

I december 2020 lade Europeiska kommissionen fram ett förslag till en ny förordning om den inre digitala marknaden inom EU; Europaparlamentets och rådets förordning om en inre marknad för digitala tjänster (rättsakten om digitala tjänster) och om ändring av direktiv 2000/31/EG[22]. Förslaget kallas även Digital Services Act, DSA.

DSA har till syfte att tydligt fastställa ansvar och ansvarsskyldighet för leverantörer av förmedlingstjänster, särskilt onlineplattformar, såsom sociala medier och marknadsplatser. Genom att fastställa tydliga krav på tillbörlig aktsamhet för vissa förmedlingstjänster, inbegripet förfaranden för anmälan och åtgärder för olagligt innehåll och möjligheten att ifrågasätta plattformarnas beslut om innehållsmodererering, syftar förslaget till att förbättra användarnas säkerhet online i hela unionen och förbättra skyddet av deras grundläggande rättigheter.[23]

I rådets allmänna inriktning[24] inför trepartsförhandlingarna mellan företrädare för Europaparlamentet, rådet och Europeiska kommissionen, framgår det av artikel 1 att DSA vare sig ska påverka tillämpningen av e-handelsdirektivet, i den föreslagna lydelsen (se nästa stycke), eller TCO-förordningen. Förslaget innebär att TCO-förordningen kommer att ha företräde framför DSA i egenskap av lex specialis.

[21] Prop. 2001/02:150 s. 98–99.
[22] Bryssel 2020-12-15, COM(2020) 825 final.
[23] Se motiveringen, särskilt s. 2.
[24] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC – General approach. Interinstitutional File: 2020/0361(COD), Brussels, den 12 november 2021, (OR. en)13613/21.

Det betyder att åtgärder mot terrorisminnehåll ska vidtas med stöd av TCO-förordningen men att vissa formella krav, till exempel avseende avlägsnandeorder, kommer att framgå av DSA.

Artikel 12–15 i e-handelsdirektivet, som bland annat innehåller ovan nämnda bestämmelser om ansvarsfrihet för värdtjänstleverantörer i vissa fall, kommer att upphöra när DSA antas (artikel 71). Motsvarande bestämmelser kommer i stället att föras in i artikel 5 DSA.

Slutligen kan här nämnas att DSA även kommer att innehålla en bestämmelse i artikel 8 som särskilt reglerar avlägsnandeorder (*orders to act against illegal content*). En order ska enligt artikeln utfärdas med stöd av nationell lagstiftning eller annan unionslagstiftning och uppfylla de generella krav som framgår av artikel 8 DSA. Det finns även ett förbud mot generell övervakning i artikel 7.

10.3.3 Förhållandet till TCO-förordningen

Utredningens bedömning: TCO-förordningen och kompletteringslagen ska inte påverka tillämpningen av e-handelsdirektivet och e-handelslagen.

TCO-förordningens förhållande till e-handelsdirektivet regleras i artikel 1.5.

> 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.

Förhållandet förtydligas ytterligare i skäl 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.

E-handelsdirektivet är implementerat i svensk rätt genom e-handelslagen. Såvitt utredningen kan överblicka bör en möjlig konflikt mellan

regelverken främst uppstå mellan TCO-förordningen och bestämmelserna om ansvarsfrihet för värdtjänstleverantörer i vissa fall. När DSA inom ett par år sannolikt kommer att antas och börja tillämpas kommer dessa bestämmelser i e-handelsdirektivet att upphöra och i stället föras in i DSA. Eftersom DSA är tänkt att, enligt det nuvarande förslaget, utgöra ett generellt ramverk bör DSA inte påverka tillämpningen av TCO-förordningen. Utredningen gör därför bedömningen att det inte finns skäl att föreslå till exempel en särskild bestämmelse i kompletteringslagen som upplyser om TCO-förordningens förhållande till e-handelslagen.

10.4 Radio- och tv-lagen

10.4.1 Allmänt om AV-direktivet

AV-direktivet[25] omfattade initialt audiovisuella medietjänster, dvs. linjära tv-sändningar och beställ-tv. En audiovisuell medietjänst definieras i AV-direktivet som en tjänst som faller under det redaktionella ansvaret hos en leverantör av medietjänster vars huvudsakliga syfte är att i informations-, underhållnings- eller utbildningssyfte tillhandahålla allmänheten program via elektroniska kommunikationsnät eller ett audiovisuellt kommersiellt meddelande (artikel 1.1.a)). AV-direktivet har huvudsakligen implementerats i svensk rätt genom radio- och tv-lagen.

År 2018 antogs ett ändringsdirektiv[26] som utvidgade direktivets tillämpningsområde till att även omfatta leverantörer av videodelningsplattformar. Samtidigt infördes bland annat en skyldighet för medlemsstaterna att säkerställa att audiovisuella medietjänster under deras jurisdiktion inte innehåller någon offentlig uppmaning att begå terroristbrott (artikel 6 i lydelsen i ändringsdirektivet). Befintliga straffbestämmelser i svensk rätt, framför allt bestämmelserna om uppvig-

[25] 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).
[26] 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 (direktivet om audiovisuella medietjänster).

ling, olaga hot och hets mot folkgrupp i brottsbalken, bedömdes uppfylla dessa skyldigheter i ändringsdirektivet.[27]

I 5:e kapitlet radio- och tv-lagen framgår krav som ställs på innehåll i audiovisuella medietjänster. De allmänna kraven på innehåll som tillhandahålls i en tv-sändning, beställ-tv eller sökbar text-tv innebär att programverksamheten som helhet ska präglas av det demokratiska statsskickets grundidéer och principen om alla människors lika värde och den enskilda människans frihet och värdighet (5 kap. 1 § radio- och tv-lagen, även kallad demokratibestämmelsen).

Tillhandahållare av tv-sändningar får enligt 5 kap. 2 § inte sända program med ingående våldsskildringar av verklighetstrogen karaktär eller med pornografiska bilder under sådan tid och på sådant sätt att det finns en betydande risk för att barn kan se programmen, om det inte av särskilda skäl ändå är försvarligt. Sådana program får inte heller tillhandahållas i beställ-tv på sådant sätt att det finns en betydande risk för att barn kan se programmen, om det inte av särskilda skäl ändå är försvarligt. Bestämmelsen genomför artikel 6 a AV-direktivet om skydd av minderåriga.

10.4.2 Leverantörer av videodelningsplattformar

Genom ändringsdirektivet utvidgades, som nämnts ovan, AV-direktivets tillämpningsområde till att även omfatta leverantörer av videodelningsplattformar. Bestämmelserna om videodelningsplattformar har implementerats i svensk rätt genom 9 a kapitlet i radio- och tv-lagen.

En videodelningsplattform är enligt 3 kap. 1 § 23 punkten radio- och tv-lagen 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.

Till skillnad från en audiovisuell medietjänst saknar en leverantör av en videodelningsplattform redaktionellt ansvar över innehållet på tjänsten. En leverantör ska för att omfattas av definitionen ha befogenhet att bestämma över hur innehållet ska organiseras på plattformen (artikel 1 i lydelsen i ändringsdirektivet).

[27] Prop. 2019/20:168 *En moderniserad radio- och tv-lag*, s. 60 f. och SOU 2019:39 *En moderniserad radio- och tv-lag – genomförande av ändringar i AV-direktivet*, s. 257 f.

I skälen till ändringsdirektivet framgår att sociala medier bör, i den utsträckning de omfattas av definitionen av en videodelningsplattformstjänst, omfattas av AV-direktivet. En förutsättning är att program och användargenererade videor utgör en väsentlig funktion i tjänsten (skäl 5). Youtube är ett exempel på en videodelningsplattform som omfattas av AV-direktivet. Youtube är en plattform som är öppen för alla, reklamfinansierad och leverantören kan inte styra vilket innehåll som användarna publicerar på tjänsten. Andra tjänster som skulle kunna vara videodelningsplattformar i direktivets mening är Facebook, Instagram, TikTok och Snapchat.

Genom ändringsdirektivet infördes en särskild skyldighet för leverantörer av videodelningsplattformar att skydda barn mot visst innehåll men även en skyldighet att skydda allmänheten från program, användargenererade videor och audiovisuella kommersiella meddelanden som innehåller till exempel uppmaning till våld, hat mot en grupp eller offentlig uppmaning till terroristbrott (artikel 28 b ändringsdirektivet). Leverantörer av videodelningsplattformar ska vidta lämpliga åtgärder för att uppfylla kravet i direktivet. Dessa bestämmelser har implementerats genom 9 a kap. 1 § och 3 § radio- och tv-lagen. I 1 § regleras särskilt ansvaret gentemot barn, där framgår följande.

> En leverantör av en videodelningsplattform ska vidta lämpliga åtgärder så att användargenererade videor, tv-program och audiovisuella kommersiella meddelanden med ingående våldsskildringar av verklighetstrogen karaktär eller med pornografiska bilder inte tillhandahålls på ett sådant sätt att det finns en betydande risk för att barn kan se dessa, om det inte av särskilda skäl ändå är försvarligt.

I 3 § uttrycks en skyldighet för leverantörer av videodelningsplattformar att vidta lämpliga åtgärder så att plattformen inte innehåller innehåll som avses i bestämmelserna om:

– olaga hot i 4 kap. 5 § brottsbalken,
– uppvigling i 16 kap. 5 § brottsbalken,
– hets mot folkgrupp i 16 kap. 8 § brottsbalken,
– barnpornografibrott i 16 kap. 10 a § brottsbalken,
– olaga våldsskildring i 16 kap. 10 c § brottsbalken, eller

– brott enligt 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.[28]

Vad som kan vara lämpliga åtgärder exemplifieras i direktivets artikel 28b.3 a–j. Lämpliga åtgärder kan till exempel vara att en leverantör inkluderar ändringsdirektivets krav i sina användarvillkor, tillhandahåller mekanismer som ger användare möjlighet att rapportera och flagga innehåll som utgör till exempel offentlig uppmaning eller att inrätta transparenta, lättanvända och ändamålsenliga klagomålsmekanismer.

Skyldigheten att vidta lämpliga åtgärder innebär inget allmänt krav på att leverantören ska övervaka innehållet på en videodelningsplattform. Bestämmelserna strider därför inte mot e-handelsdirektivets övervakningsförbud (skäl 48 ändringsdirektivet).

Myndigheten för press, radio och tv har tillsyn över bland annat bestämmelserna i 9 a kap. 1 § och 3 § radio- och tv-lagen och får besluta om de förelägganden som behövs för att en leverantör av en videodelningsplattform ska uppfylla kraven på lämpliga åtgärder i radio- och tv-lagen. Ett sådant föreläggande får myndigheten förena med vite (16 kap. 3 § och 17 kap. 11 a § radio- och tv-lagen).

10.4.3 Förhållandet till TCO-förordningen

Utredningens förslag: En ny bestämmelse bör införas i 9 a kap. radio- och tv-lagen. Bestämmelsen ska upplysa om att 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.

I detta avsnitt analyserar utredningen förhållandet mellan AV-direktivet och TCO-förordningen. Utgångspunkten för bedömningen är ordalydelsen av artikel 1.5 i TCO-förordningen.

[28] I prop. 2021/22:133 s. 46 föreslås vissa ändringar av bestämmelsen till följd av förslaget om en ny terroristbrottslag.

> 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.

Förhållandet mellan rättsakterna förtydligas ytterligare i skäl 8 TCO-förordningen.

> 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.

TCO-förordningen utgår således från att förordningen inte ska påverka tillämpningen av AV-direktivet. Detta innebär att inte heller bestämmelserna i radio- och tv-lagen bör påverkas när TCO-förordningen börjar tillämpas.

Utredningens bedömning är att terrorisminnehåll kan spridas via en tjänst som omfattas av både AV-direktivet (radio- och tv-lagen) och TCO-förordningen. Frågan är om, och i så fall vilka, tillämpningsproblem som kan uppstå om terrorisminnehåll sprids på en tjänst som omfattas av båda regelverken.

När det kommer till möjligheten att utfärda avlägsnandeorder med stöd av TCO-förordningen, saknar detta motsvarighet i AV-direktivet respektive radio- och tv-lagen. Beslut om avlägsnandeorder och beslut om sanktioner vid underlåtenhet att följa en avlägsnandeorder bör därför enligt utredningens bedömning inte leda till något problem vid tillämpningen av regelverken.

Både TCO-förordningen och AV-direktivet innehåller dock skyldigheter för tillhandahållare av audiovisuella medietjänster, leverantörer av videodelningsplattformar respektive värdtjänstleverantörer som innebär att aktörerna ska organisera sina tjänster så att inte skadligt eller olagligt innehåll, till exempel terrorisminnehåll, sprids till allmänheten. Skyldigheterna är något olika utformade i rättsakterna. I radio- och tv-lagen finns ett krav på att vidta ”lämpliga åtgärder” (se till exempel 9 a kap. 1 §) och i TCO-förordningen ett krav på att vidta ”specifika åtgärder” (artikel 5).

Om terrorisminnehåll sprids i audiovisuella medietjänster framgår det av TCO-förordningen att bestämmelserna i AV-direktivet har företräde framför TCO-förordningen. Det innebär att radio- och

tv-lagens bestämmelser har företräde framför TCO-förordningen och kompletteringslagen. Såvitt utredningen kan bedöma bör en konflikt främst uppstå om terrorisminnehåll sprids via beställ-tv. En tillhandahållare av audiovisuella medietjänster vars tjänster missbrukas för spridning av terrorisminnehåll ska dock, även om TCO-förordningen inte är tillämplig, fortfarande uppfylla kraven i radio- och tv-lagen.

Om terrorisminnehåll i stället sprids via en videodelningsplattform kan förhållandet mellan AV-direktivet, radio- och tv-lagen och TCO-förordningen vara ett annat. Utgångspunkten är dock den samma, att en leverantör av en videodelningsplattform alltid ska vidta lämpliga åtgärder för att uppfylla kraven i 9 a kap. radio- och tv-lagen. Men som framgår av skäl 8 TCO-förordningen ska AV-direktivets bestämmelser om leverantörer av videodelningsplattformar inte påverka de särskilda skyldigheter som följer av TCO-förordningen. Det innebär att en leverantör av en videodelningsplattform som anses exponerad för terrorisminnehåll enligt artikel 5.4 TCO-förordningen också ska uppfylla de särskilda krav som följer av artikel 5 i TCO-förordningen. Skulle en leverantör inte uppfylla kraven kan den behöriga myndigheten besluta om sanktioner med stöd av TCO-förordningen och kompletteringslagen.

Myndigheten för press, radio och tv utövar tillsyn över bestämmelserna i 9 a kap. radio- och tv-lagen och en annan myndighet, enligt utredningens förslag Polismyndigheten, kommer att vara behörig myndighet enligt TCO-förordningen. När TCO-förordningen börjar tillämpas kan utredningen se fördelar med att de båda myndigheterna upprättar kanaler för samverkan i frågor som rör leverantörer av videodelningsplattformar.

För att underlätta tillämpningen av radio- och tv-lagen och TCO-förordningen bedömer utredningen att det finns anledning att föreslå en bestämmelse i 9 a kap. radio- och tv-lagen som upplyser om förhållandet till TCO-förordningen och kompletteringslagen. En sådan bestämmelse bör underlätta för såväl tillämpande myndigheter som för de leverantörer av videodelningsplattformar som kan komma att omfattas av regelverken.

11 Konsekvenser av utredningens förslag

11.1 Allmänna utgångspunkter

Utredningen ska redovisa vilka konsekvenser i olika avseenden som förslagen i betänkandet kan få (1 § andra stycket kommittéförordningen [1998:1474]). Om förslagen påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska utredningen redovisa en beräkning av dessa konsekvenser i betänkandet (14 §). Innebär förslagen samhällsekonomiska konsekvenser i övrigt ska utredningen även redovisa dessa. Om utredningens förslag leder till kostnadsökningar eller intäktsminskningar för staten, kommuner eller regioner ska utredningen föreslå hur förslagen ska finansieras.

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

Utöver kraven som följer av kommittéförordningen lyfter utredningens direktiv (dir. 2021:24) särskilt fram att utredningen ska redovisa hur eventuella kostnadsökningar för det allmänna ska finansieras. Utredningen ska vidare redovisa förslagens konsekvenser för brottsbekämpningen och säkerställa att förslagen är förenliga med grundläggande fri- och rättigheter. Slutligen ska utredningen redovisa förslagens konsekvenser för företagen.

De förslag som utredningen lämnar i betänkandet syftar till att uppfylla kraven i TCO-förordningen och säkerställa att förordningen får ett effektivt genomslag i svensk rätt. För att förordningen ska få önskat genomslag har utredningen sett ett behov av ett antal kompletteringar och ändringar i svensk rätt. Sammanfattningsvis föreslår utredningen i detta slutbetänkande ett nationellt sanktionssystem vid överträdelser av TCO-förordningen, bestämmelser om överklagande, författningsändringar i radio- och tv-lagen och BBS-lagen samt en bestämmelse om sekretess för vissa uppgifter hos Polismyndigheten och en reglerad uppgiftsskyldighet mellan Polismyndigheten och Säkerhetspolisen.

I detta kapitel redovisar utredningen sin bedömning av vilka konsekvenser förslagen kan få i olika avseenden. Utredningen har i betänkandet utgått, och utgår även i denna analys, från antagandet att Polismyndigheten kommer att utses till behörig myndighet enligt TCO-förordningen.

11.2 Vilka berörs av utredningens förslag?

Utredningens förslag berör framför allt den myndighet som utses till behörig myndighet för Sveriges räkning. Som framgått ovan har utredningen föreslagit att Polismyndigheten bör utses till behörig myndighet.

Förslagen kan även beröra andra myndigheter som kan komma att samverka med den behöriga myndigheten, till exempel Säkerhetspolisen, Totalförsvarets forskningsinstitut och Centrum mot våldsbejakande extremism vid Brottsförebyggande rådet.

Bestämmelserna om sanktioner och om rätten att överklaga beslut som meddelas med stöd av TCO-förordningen eller kompletteringslagen gör att även de allmänna förvaltningsdomstolarna och Kronofogdemyndigheten kan komma att beröras av utredningens förslag.

Slutligen kommer även enskilda personer och juridiska personer beröras av bestämmelserna i TCO-förordningen och kompletteringslagen i den mån de omfattas av begreppet värdtjänstleverantör och har en värdtjänst som missbrukas för spridning av terrorisminnehåll.

11.2.1 Polismyndigheten

Utredningen har arbetat utifrån hypotesen att Polismyndigheten kommer att utses till behörig myndighet. Utredningens bedömning nedan utgår därför från att det är Polismyndigheten som ska utföra uppgifterna i TCO-förordningen.

Konsekvenserna för den behöriga myndigheten är i huvudsak en följd av antagandet av TCO-förordningen och inte av utredningens förslag. Uppgifterna som den behöriga myndigheten ska utföra enligt TCO-förordningen består i att utfärda avlägsnandeorder, granska avlägsnandeorder, övervaka genomförandet av specifika åtgärder och påföra sanktioner. En särskild kontaktpunkt ska inrättas eller utses vid myndigheten (artikel 12.2 TCO-förordningen). Bestämmelserna om avlägsnandeorder och granskning av gränsöverskridande order kräver att det finns en dygnet runt bemannad kontaktpunkt vid Polismyndigheten som kan ta emot inkommande ärenden och vidarebefordra utgående information. Utredningen bedömer därför att de nya uppgifterna innebär ett ökat administrativt arbete som kommer att resultera i ökade kostnader för Polismyndigheten. Initialt kommer det finnas behov av att utbilda personal och att skapa nya arbetsformer och rutiner för handläggning av TCO-ärenden. Kostnaderna i denna del får emellertid bedömas som begränsade.

Frågan är hur stor arbetsbörda den löpande tillämpningen av TCO-förordningen kommer att innebära för den behöriga myndigheten. Utgångspunkten är att den behöriga myndigheten i Sverige kommer att ha jurisdiktion över värdtjänstleverantörer som är etablerade eller har sin rättsliga företrädare registrerad i landet och att myndigheten ska övervaka dessa värdtjänstleverantörers genomförande av specifika åtgärder (artikel 5) samt påföra sanktioner vid överträdelser av TCO-förordningen (artikel 18). Den behöriga myndigheten i Sverige kan dock utfärda en avlägsnandeorder mot en värdtjänstleverantör oavsett om leverantören är etablerad inom eller utanför Sverige (se artikel 3 och 16).

En bedömning av antalet ärenden som Polismyndigheten kan komma att handlägga är beroende av ett antal faktorer som är osäkra. Utredningen berörde dessa faktorer redan i delbetänkandet. Det som försvårar bedömningen är att TCO-förordningen ännu inte har börjat att tillämpas i EU och att den saknar tidigare motsvarighet. Mängden ärenden kommer att vara beroende av bland annat hur begreppet

värdtjänstleverantör kommer att tolkas och vilken ambitionsnivå den behöriga myndigheten kommer att arbeta utifrån. Myndighetens arbetsbörda kommer också att påverkas av i vilken utsträckning andra medlemsstater kommer att tillämpa TCO-förordningen och hur de kommer att förhålla sig till material som publiceras av innehållsleverantörer eller värdtjänstleverantörer som är etablerade i Sverige. Flera medlemsstater har uppgett att de kommer att fortsätta använda frivilliga *referrals* även när TCO-förordningen börjar tillämpas. Utredningen gör mot denna bakgrund bedömningen att den behöriga myndigheten i Sverige inte kommer att handlägga några större mängder av gränsöverskridande order.

Polismyndigheten har fått tillfälle att till utredningen själva uppge vilka konsekvenser myndigheten bedömer att ett uppdrag som behörig myndighet kan innebära för myndigheten. Polismyndigheten har uppgett att uppgifterna i TCO-förordningen är helt nya uppgifter för myndigheten både såvitt gäller att utfärda avlägsnandeorder, utföra tillsynsuppgifter och möjligheten att besluta om sanktioner. Uppdraget och utredningens förslag kommer att kräva kompetensutveckling och en organisation som kan ta emot, handlägga och besluta i TCO-ärenden. Polismyndigheten har haft svårt att i dagsläget ange i vilken utsträckning uppdraget kommer att innebära en kostnadsökning för myndigheten.

I delbetänkandet bedömde utredningen att det saknades förutsättningar för utredningen att göra en annan bedömning än att uppdraget ryms inom Polismyndighetens befintliga ekonomiska ram. De osäkerhetsfaktorer som utredningen då redogjorde för kvarstår. Utredningen gör därför samma bedömning som i delbetänkandet, att uppdraget som behörig myndighet ryms inom Polismyndighetens befintliga ekonomiska ramar. Om det skulle visa sig att uppdraget innebär större ekonomiska konsekvenser än vad utredningen nu kan överblicka har Polismyndigheten möjlighet att återkomma inom ramen för myndighetens ordinarie budgetdialoger.

Det ska även tilläggas att det inom några år sannolikt kommer att antas fler rättsakter inom EU som berör innehåll på internet och värdtjänstleverantörer. Liksom utredningen berörde i delbetänkandet finns det då anledning att göra en översyn av den behöriga myndighetens uppdrag. En översyn skulle kunna resultera i att vissa uppgifter i TCO-förordningen, särskilt sådana som är av mer administrativ karaktär eller av tillsynskaraktär, lyfts bort från Polismyndigheten. En sådan

förändring bör få som konsekvens att uppgiften som behörig myndighet kommer att ta mindre resurser i anspråk hos Polismyndigheten.

11.2.2 Säkerhetspolisen och andra samverkansmyndigheter

Utredningen har bedömt att Polismyndigheten kan behöva samverka med andra myndigheter i vissa frågor, till exempel rörande kunskap om miljöer och aktörer som kan kopplas ihop med terrorism. Det bör främst handla om information som Säkerhetspolisen besitter i sin egenskap av ansvarig för terrorbekämpningen i Sverige.

Den förväntade samverkan i TCO-ärenden bedöms som begränsad till några frågor. I ett initialt skede kan utredningen föreställa sig att kunskapsinhämtning från Säkerhetspolisen sker i större omfattning. Detta är dock alltjämt beroende av mängden ärenden som Polismyndigheten kommer att handlägga. Utredningens bedömning är att Säkerhetspolisens och andra myndigheters samverkan med den behöriga myndigheten inom ramen för TCO-förordningen och kompletteringslagen inte kommer att innebära en större belastning än att uppgiften ryms inom befintliga anslag.

11.2.3 Övriga myndigheter

Utredningen föreslår ett sanktionssystem vid överträdelser av TCO-förordningen som innehåller bestämmelser om sanktionsavgifter och vitesföreläggande. Bestämmelserna kan komma att generera enstaka ärenden hos Kronofogdemyndigheten. Uppgiften kan hanteras inom myndighetens befintliga anslag.

Utredningen föreslår också att beslut som den behöriga myndigheten meddelar med stöd av TCO-förordningen och kompletteringslagen ska få överklagas till allmän förvaltningsdomstol. Utöver de beslut som överklagas till domstolen kommer måltillströmningen även att bestå av ansökan om utdömande av vite. Det kommer med all säkerhet att röra sig om enstaka mål varför uppgiften bör rymmas inom domstolarnas befintliga anslag.

11.2.4 Värdtjänstleverantörer

TCO-förordningen och kompletteringslagen innehåller skyldigheter för värdtjänstleverantörer vars värdtjänster missbrukas för spridning av terrorisminnehåll.

En återkommande fråga under utredningens arbete har varit vilka och hur många svenska aktörer som i praktiken kommer att omfattas av begreppen värdtjänst och värdtjänstleverantör i TCO-förordningen och utredningens förslag. Frågan har särskild betydelse för bedömningen av vilka konsekvenser utredningens förslag kan få för branschen, men den påverkar även hur stor arbetsbörda som den behöriga myndigheten kommer att få.

Utredningen har varit i kontakt med företrädare för tech-branschen. Dessa har haft svårt att utifrån ordalydelsen i TCO-förordningen ange en uppfattning om hur många aktörer i Sverige som kan beröras av TCO-förordningen och utredningens förslag. Branschorganisationen TechSverige har uttryckt att de inte kan lämna någon konkret uppgift. Antalet aktörer som berörs av TCO-förordningen kommer att bero på hur definitionen kommer att tolkas. Inte heller Internetstiftelsen har kunnat uppskatta hur många värdtjänstleverantörer som kan komma att omfattas av regleringen.

Utredningen har problematiserat begreppen värdtjänst och värdtjänstleverantör i avsnitt 4.3.4. Den slutsats som utredningen kan dra utifrån ordalydelsen i TCO-förordningen är att det är svårt att på förhand ange vilka värdtjänstleverantörer som kommer att träffas av skyldigheterna i förordningen. Det återstår att se när TCO-förordningen börjar att tillämpas hur begreppen, och i förlängningen TCO-förordningen, kommer att tillämpas och tolkas inom unionen.

När det kommer till antalet leverantörer av videodelningsplattformar, en aktör som kan omfattas av TCO-förordningen, kan utredningen hämta viss ledning från en kartläggning som Myndigheten för press, radio och tv gjorde på uppdrag av 2018 års AV-utredning i anledning av genomförandet av ändringsdirektivet till AV-direktivet.[1] Myndigheten fick i uppdrag att översiktligt beskriva marknaden för videodelningsplattformstjänster och genomföra en kartläggning av sådana potentiella tjänster under svensk jurisdiktion. Myndigheten identifierade två segment där potentiella svenska videodelningsplatt-

[1] ”Videodelningsplattformar i Sverige”, Myndigheten för press, radio och tv, dnr 19/01054. Se även *En moderniserad radio- och tv-lag – Genomförande av ändringar i AV-direktivet* (SOU 2019:37) och prop. 2019/20:168 *En moderniserad radio- och tv-lag*.

formar figurerar; intresseforum med möjlighet till videodelning och videodelningsplattformar för streaming av sport. Inom dessa två segment fann myndigheten i respektive segment tre potentiella svenska leverantörer av videodelningsplattformar.

Utredningen har varit i kontakt med Myndigheteten för press, radio och tv för att efterhöra om myndigheten har någon uppfattning om hur branschen utvecklats och förändrats under åren som passerat efter kartläggningen. Myndigheten har uppgett till utredningen att det är svårt att kartlägga videodelningsplattform-branschen. Ingen plattform är i dag registrerad hos myndigheten. Myndighetens uppfattning är att de slutsatser som drogs i den tidigare kartläggningen alltjämt gäller. Branschen har inte genomgått någon större förändring till antal. De flesta videodelningsplattformar som används i Sverige är etablerade utanför landet. Myndigheten har identifierat två trender; fler plattformar för streaming av sport håller på att utvecklas och företag med webbshopping har börjat att kombinera sina tjänster med liveshopping tillsammans med olika influensers.

Utredningens bedömning är att det inte går att uppge hur många enskilda och juridiska personer som kommer att beröras av TCO-förordningen och kompletteringslagen. Svårigheten har framför allt sin grund i den osäkerhet som finns kring tolkningen av begreppen värdtjänst och värdtjänstleverantör. Det är därtill en bransch under ständig utveckling och det uppstår hela tiden nya tjänster och tekniska lösningar som kan öka eller minska antalet aktörer som eventuellt kan definieras som värdtjänstleverantörer. Flertalet av de större värdtjänstleverantörer som många använder i Sverige, till exempel Facebook, Instagram och TikTok är inte etablerade här i landet och kommer sannolikt inte att registrera en rättslig företrädare här. Rörande leverantörer av videodelningsplattformar talar kartläggningen av Myndigheten för press, radio och tv för att det endast är ett fåtal som är etablerade i landet.

För de värdtjänstleverantörer som kommer att omfattas av TCO-förordningen och kompletteringslagen får regelverken de konsekvenser som framgår av betänkandet.

11.3 Konsekvenser för brottsbekämpningen

Utredningen ska även överväga vilka konsekvenser utredningens förslag kan få för brottsbekämpningen. TCO-förordningen och kompletteringslagen ger den behöriga myndigheten verktyg att vidta åtgärder för att motverka spridningen av terrorisminnehåll på internet. Åtgärderna i TCO-förordningen är en del av EU:s arbete mot terrorism. Det handlar främst om att minska risken för att enskilda individer radikaliseras genom material på internet, att potentiella gärningspersoner kan införskaffa instruktioner på internet och att terrorattentat livesänds och glorifieras på internet.

Utredningens förslag ska bland annat bidra till att TCO-förordningen får ett effektivt genomslag i svensk rätt och därmed öka möjligheterna att uppnå det önskade syftet; att motverka spridning av terrorisminnehåll på internet och i förlängningen öka säkerheten i unionen. Utredningens bedömning är att TCO-förordningen i sig kommer att leda till positiva effekter för brottsbekämpningen både ur ett europeiskt och ett svenskt perspektiv.

Utöver de direkta effekterna av åtgärder som vidtas med stöd av TCO-förordningen och kompletteringslagen bör hanteringen av TCO-ärenden också leda till att information som Polismyndigheten får kännedom om i ett ärende enligt TCO-förordningen kan vidarebefordras till den brottsbekämpande verksamheten inom Polismyndigheten eller Säkerhetspolisen. Ett sådant informationsutbyte inom och mellan myndigheterna bör också leda till positiva effekter för brottsbekämpningen.

11.4 Övriga konsekvenser

Utredningen har i avsnitt 5 analyserat TCO-förordningens och kompletteringslagens förhållande till skyddet för yttrande- och informationsfrihet i regeringsformen och yttrandefrihetsgrundlagarna. En tydlig utgångspunkt är att TCO-förordningen och kompletteringslagen inte ska tillämpas på innehåll som omfattas av grundlagsskyddet.

Genom möjligheten att överklaga den behöriga myndighetens beslut till allmän förvaltningsdomstol säkerställs enskilda och juridiska personers rätt till effektiva rättsmedel.

12 Författningskommentar

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

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.

Paragrafen reglerar lagens tillämpningsområde. Övervägandena finns i avsnitt 7.1.

Av bestämmelsen framgår att syftet med lagen är att komplettera Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online, i fortsättningen kallad TCO-förordningen. Eftersom lagen kompletterar TCO-förordningen ska den läsas tillsammans med förordningen.

Hänvisningar till förordningen är i huvudsak dynamiska. Det innebär att hänvisningen avser TCO-förordningen i den vid varje tidpunkt gällande lydelsen. På så sätt säkerställs att ändringar i TCO-förordningen får genomslag i lagen och att den nationella rättstillämpningen vid varje tillfälle kommer att överensstämma med kraven i förordningen. I 4 § och 6 § görs dock hänvisning till TCO-förordningen i dess ursprungliga lydelse. Det innebär att dessa bestämmelser i stället innehåller en statisk hänvisning till förordningen, dvs. förordningens lydelse i den ursprungliga versionen gäller vid tillämpning.

2 §

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

Övervägandena finns i avsnitt 7.1.

En uppräkning av definitioner finns i artikel 2 i TCO-förordningen.

Behörig myndighet

3 §

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

Övervägandena finns i delbetänkandet *EU:s förordning om terrorisminnehåll på internet – frågan om behörig myndighet* (SOU 2021:76), se särskilt avsnitt 6.

Medlemsstaterna ska utse den eller de behöriga myndigheter som ska utföra de uppgifter som följer av artikel 12 i 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.

Artikel 18 i TCO-förordningen anger att medlemsstaterna ska fastställa nationella regler om sanktioner vid överträdelser av vissa däri uppräknade artiklar.

I bestämmelsen ges den behöriga myndigheten en möjlighet att rikta ett vitesföreläggande mot en värdtjänstleverantör som åsidosätter vissa uppräknade skyldigheter i TCO-förordningen. Övervägandena finns i avsnitt 8.5, se särskilt 8.5.4.

Vilka aktörer som ska anses vara värdtjänstleverantör i förordningens mening följer av definitionen i artikel 2 TCO-förordningen, se även avsnitt 4.3.4.

Enligt huvudregeln 1 § förvaltningslagen (2017:900) ska myndigheten som handlägger ett ärende om föreläggande enligt bestämmelsen tillämpa förvaltningslagen.

I *punkterna 1–8* framgår vilka åsidosättanden av TCO-förordningen som kan utgöra skäl för den behöriga myndigheten att utfärda ett föreläggande. I *punkterna 6 och 7* är ett åsidosättande av skyldigheterna i TCO-förordningen för handen först när tidsfristerna i respektive artikel löpt ut.

I *andra stycket* framgår att ett föreläggande som den behöriga myndigheten utfärdar med stöd av första stycket får förenas med ett vite. Den behöriga myndigheten avgör när ett föreläggande ska förenas med vite. Ett föreläggande bör förenas med vite när det kan befaras att värdtjänstleverantören inte kommer att följa det utfärdade föreläggandet.

5 §

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

Övervägandena framgår av avsnitt 8.5.5.

Bestämmelsen i paragrafen hänvisar till den inte uttömmande uppräkningen av omständigheter i artikel 18.2 i TCO-förordningen som den behöriga myndigheten ska ta hänsyn till när vitets storlek bestäms i det enskilda fallet. Även andra relevanta omständigheter än de som framgår av artikeln kan beaktas.

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 om att terrorisminnehåll har avlägsnats eller att terrorisminnehåll gjorts oåtkomligt i enlighet med 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).

Medlemsstaterna ska fastställa regler om sanktioner för överträdelser av de artiklar som räknas upp i artikel 18 TCO-förordningen. I paragrafen ges den behöriga myndigheten möjlighet att vid vissa däri uppräknade överträdelser av TCO-förordningen påföra en värdtjänstleverantör en sanktionsavgift. Övervägande finns i avsnitt 8.5.7 och 8.5.8.

Vilka aktörer som omfattas av begreppet värdtjänstleverantör följer av definitionen i artikel 2 TCO-förordningen. Bestämmelsen genomför, tillsammans med möjligheten i 4 § att utfärda vitesföreläggande, artikel 18 i TCO-förordningen.

I *punkterna 1–7* framgår vilka överträdelser av TCO-förordningen som kan föranleda att sanktionsavgift påförs en värdtjänstleverantör. Beslut om sanktionsavgift fattas av den behöriga myndigheten. Det krävs inte att myndigheten kan konstatera uppsåt eller vårdslöshet hos den värdtjänstleverantör som gjort sig skyldig till överträdelsen. Ansvaret är strikt när en överträdelse konstaterats.

Av 8 § följer att när den behöriga myndigheten bestämmer sanktionsavgiftens storlek ska myndigheten beakta de omständigheter som framgår av artikel 18.2 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 i enlighet med artikel 18.3 i TCO-förordningen.

Övervägandena finns i avsnitt 8.5.9.

I *första stycket* anges inom vilket beloppsintervall som en sanktionsavgift ska bestämmas. Det är den behöriga myndigheten som beslutar om sanktionsavgiftens storlek. Hur avgiften ska bestämmas i det enskilda fallet regleras i 8 §.

Andra stycket reglerar hur storleken på en sanktionsavgift ska bestämmas vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheten i artikel 3.3 TCO-förordningen. Artikel 3.3 innehåller skyldigheten 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. Vid en systematisk eller fortgående underlåtenhet att verkställa avlägsnandeorder ska sanktionsavgiften, utan hinder av första stycket, enligt artikel 18.3 TCO-förordningen uppgå till maximalt fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret.

8 §

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

Övervägandena framgår av avsnitt 8.5.10.

Bestämmelsen hänvisar till den inte uttömmande uppräkningen av omständigheter i artikel 18.2 i TCO-förordningen som den behöriga myndigheten ska ta hänsyn till när avgiftens storlek bestäms i det enskilda fallet. Även andra relevanta omständigheter kan beaktas.

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.

Övervägandena finns i avsnitt 8.5.11.

Första stycket innebär att kommunikation enligt 25 § förvaltningslagen med den värdtjänstleverantör som avgiften ska tas ut av ska ha skett inom två år från den dag då överträdelsen ägde rum, annars får den behöriga myndigheten inte besluta om en sanktionsavgift. Bevisbördan för att kommunikation har skett ligger på den behöriga myndigheten.

Av *andra stycket* framgår att ett beslut om sanktionsavgift ska delges. Det innebär att den behöriga myndigheten ska använda de metoder för delgivning som regleras i delgivningslagen (2010:1932).

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.

Övervägandena finns i avsnitt 8.5.11.

Paragrafen anger när och till vilken myndighet en sanktionsavgift ska betalas samt vad myndigheten ska iaktta om avgiften inte betalas i tid.

11 §

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

Övervägandena finns i avsnitt 8.5.11.

Paragrafen innehåller en bestämmelse om när en beslutad sanktionsavgift inte längre behöver betalas.

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.

Övervägandena finns i avsnitt 9.4.2.

Paragrafen innehåller en sekretessbrytande uppgiftsskyldighet. *Första stycket* innehåller en skyldighet för Säkerhetspolisen att lämna ut sekretesskyddade uppgifter till den behöriga myndigheten, till exempel uppgifter som den behöriga myndigheten kan behöva för att bedöma om visst innehåll utgör terrorisminnehåll (se 10 kap. 28 § offentlighets- och sekretesslagen [2009:400], OSL).

I *andra stycket* får Säkerhetspolisen motsvarande rätt att ta del av uppgifter från den behöriga myndigheten som är sekretesskyddade. Det kan vara uppgifter som Säkerhetspolisen behöver för att kunna bistå den behöriga myndigheten enligt första stycket, till exempel innehåll som misstänks utgöra terrorisminnehåll.

Uppgiftsskyldigheten gäller inom ramen för TCO-förordningen och denna lag. Bestämmelsen är utformad som en skyldighet och utgångspunkten är att uppgifter ska lämnas ut. Det är den utlämnande myndigheten som prövar om förutsättningarna för utlämnande är uppfyllda. I *tredje stycket* kan en myndighet besluta att inte lämna ut en uppgift om det framkommer särskilda skäl däremot. Det är den utlämnande myndigheten som prövar om det finns särskilda skäl mot att lämna ut en uppgift.

En uppgiftsskyldighet som grundas på 10 kap. 28 § OSL får i vissa andra fall inte tillämpas. Det handlar främst om utlämnande av uppgifter som härrör från internationella avtal, se till exempel 15 kap. 1 a §, 27 kap. 5 § och 34 kap. 4 § OSL.

Överklagande

13 §

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

Prövningstillstånd krävs vid överklagande till kammarrätten.

Övervägandena finns i avsnitt 7.3 och 8.5.13.

Paragrafen reglerar rätten att överklaga ett beslut som meddelats av den behöriga myndigheten med stöd av TCO-förordningen eller denna lag. Endast den som ett beslut har gått emot är klagoberättigad, dvs. har rätt att överklaga.

Bestämmelsen genomför rätten till rättsmedel i artikel 9 TCO-förordningen. Det innebär att en värdtjänstleverantör som har mottagit en avlägsnandeorder eller ett annat beslut som meddelats av den behöriga myndigheten med stöd av TCO-förordningen eller denna lag har rätt att överklaga beslutet till allmän förvaltningsdomstol. Motsvarande rätt till domstolsprövning har även en innehållsleverantör vars innehåll berörs av en avlägsnandeorder enligt artikel 3.1 TCO-förordningen eller ett beslut enligt artikel 4.4 TCO-förordningen.

Ikraftträdande

Lagen ska gälla från den 1 juli 2023. Överväganden finns i avsnitt 7.4.

12.2 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, 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.

Paragrafen innehåller en uppräkning av undantag från lagens tillämpningsområde. En ändring har gjorts i paragrafen genom ett tillägg av

punkten 5. Punkten 5 innehåller en bestämmelse som innebär att lagen inte är tillämplig på meddelanden som omfattas av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen). Övervägandena finns i avsnitt 10.2.

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

Paragrafen anger att den som tillhandahåller en tjänst för elektronisk förmedling av meddelanden (elektronisk anslagstavla) i vissa fall ska ta bort eller på annat sätt förhindra vidare spridning av ett insänt meddelande.

En ändring har gjorts i första stycket första punkten i anledning av genomförandet av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorism-

innehåll online. Hänvisningen till brottet offentlig uppmaning i 3 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (rekryteringslagen), tas bort. Om innehållet i ett meddelande utgör offentlig uppmaning kan i stället TCO-förordningen och lagen med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online bli tillämpliga. Övervägandena finns i avsnitt 10.2.

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 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.

Paragrafen reglerar bland annat straffansvar för den som bryter mot skyldigheten i 5 § att ta bort vissa meddelanden.

I andra stycket har en ändring gjorts. Hänvisningen till rekryteringslagen tas bort till följd av genomförandet av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online. Övervägandena finns i avsnitt 10.2.

Ikraftträdande

Lagen ska gälla från den 1 juli 2023. Överväganden finns i avsnitt 7.4.

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

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 enskilds 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.

Överväganden finns i avsnitt 9.4.1.

Paragrafen är ny och innehåller i *första stycket* en bestämmelse till skydd för uppgifter om enskilds personliga och ekonomiska förhållanden som förekommer hos Polismyndigheten i ett ärende enligt 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.

Bestämmelsen har utformats med ett rakt skaderekvisit vilket innebär att det finns en presumtion för att en uppgift i ett ärende är offentlig.

I *andra stycket* framgår att för uppgifter om enskilds personliga eller ekonomiska förhållanden i en allmän handling gäller sekretess i högst sjuttio år.

Ikraftträdande

Lagen ska gälla från den 1 juli 2023. Överväganden finns i avsnitt 7.4.

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

9 a kap.

14 §

För leverantörer av videdelningsplattformar 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.

Bestämmelserna i kapitlet genomför huvudsakligen 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, AV-direktivet) och innehåller olika skyldigheter för leverantörer av videodelningsplattformar.

Även Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (TCO-förordningen) och lagen (SFS 2023:xx) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online (kompletteringslagen) innehåller vissa skyldigheter som kan komma att omfatta en leverantör av videodelningsplattformar.

TCO-förordningen och kompletteringslagen är tillämplig på värdtjänstleverantörer, definitionen av begreppet framgår av artikel 2 TCO-förordningen. En leverantör av videodelningsplattformar kan komma att omfattas av begreppet värdtjänstleverantör i TCO-förordningen.

I 9 a kap. radio- och tv-lagen framgår att en leverantör av videodelningsplattformar i vissa fall är skyldiga att vidta lämpliga åtgärder. En motsvarande skyldighet att vidta specifika åtgärder följer av artikel 5 i TCO-förordningen för en värdtjänstleverantör som anses exponerad för terrorisminnehåll. Det kan uppkomma situationer när en leverantör av videodelningsplattformar anses exponerad för terrorisminnehåll enligt artikel 5.4 TCO-förordningen och därför

också måste uppfylla de särskilda krav som följer av artikel 5 i TCO-förordningen (se artikel 1.5 och skäl 8 TCO-förordningen).

Paragrafen som är ny innehåller en bestämmelse som upplyser om förhållandet till TCO-förordningen och lagen (2023:xx) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll.

Övervägandena finns i avsnitt 10.4.

Ikraftträdande

Lagen ska gälla från den 1 juli 2023. Överväganden finns i avsnitt 7.4.

Kommittédirektiv 2021:24

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

Beslut vid regeringssammanträde den 15 april 2021

Sammanfattning

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

Utredaren ska bl.a.

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

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

EU-förordningen

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

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

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

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

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

Den nuvarande svenska regleringen

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

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

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

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

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

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

Uppdraget att föreslå behörig myndighet

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

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

Utredaren ska därför

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

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

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

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

Utredaren ska därför

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

Konsekvensbeskrivningar

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

Kontakter och redovisning av uppdraget

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

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

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

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

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

(Justitiedepartementet)

17.5.2021 SV Europeiska unionens officiella tidning L 172/79

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2021/784

av den 29 april 2021

om åtgärder mot spridning av terrorisminnehåll online

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

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

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande [1],

i enlighet med det ordinarie lagstiftningsförfarandet [2], och

av följande skäl:

(1) Denna förordning syftar till att säkerställa att den digitala inre marknaden fungerar smidigt i ett öppet och demokratiskt samhälle, genom att motverka att värdtjänster missbrukas för terrorismändamål samt bidra till den allmänna säkerheten i hela unionen. Den digitala inre marknadens funktion bör förbättras genom att rättssäkerheten ökas för värdtjänstleverantörer och användarnas förtroende för onlinemiljön stärks, samt genom att skyddet för yttrandefriheten förbättras, inbegripet friheten att ta emot och sprida information och idéer i ett öppet och demokratiskt samhälle och mediernas frihet och mångfald.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(16) En betydande anknytning till unionen bör föreligga om värdtjänstleverantören har ett verksamhetsställe i unionen, om dess tjänster används av ett betydande antal användare i en eller flera medlemsstater, eller om dess verksamhet riktas till en eller flera medlemsstater. Huruvida verksamheten är riktad till en eller flera medlemsstater bör avgöras på grundval av samtliga relevanta omständigheter, inbegripet faktorer som användning av ett språk eller en valuta som i allmänhet används i den berörda medlemsstaten, eller möjligheten att beställa varor eller tjänster från medlemsstaten. En sådan riktad karaktär skulle också kunna härröra från det faktum att en app finns tillgänglig i berörd nationell appstore, att lokal marknadsföring eller reklam görs på ett språk som vanligen används i den berörda medlemsstaten eller att kundkontakter, såsom kundtjänst, sköts på ett språk som vanligen används i den medlemsstaten. En betydande anknytning bör också antas föreligga om en värdtjänstleverantör riktar sin verksamhet till en eller flera medlemsstater i den mening som avses i artikel 17.1 c i Europaparlamentets och rådets förordning (EU) nr 1215/2012 ([8]). Enbart det faktum att en värdtjänstleverantörs webbplats, en e-postadress eller andra kontaktuppgifter är tillgängliga i en eller flera medlemsstater bör inte i sig vara tillräckligt för att utgöra en betydande anknytning. Dessutom bör det inte kunna anses föreligga en betydande anknytning till unionen på grund av att en tjänst tillhandahålls i det enda syftet att efterleva det förbud mot diskriminering som fastställs i Europaparlamentets och rådets förordning (EU) 2018/302 ([9]).

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

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

([9]) Europaparlamentets och rådets förordning (EU) 2018/302 av den 28 februari 2018 om åtgärder mot omotiverad geoblockering och andra former av diskriminering på grund av kunders nationalitet, bosättningsort eller etableringsort på den inre marknaden och om ändring av förordningarna (EG) nr 2006/2004 och (EU) 2017/2394 samt direktiv 2009/22/EG (EUT L 60 I, 2.3.2018, s. 1).

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

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

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

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

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

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

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

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

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

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

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

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

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

(30) Transparens i värdtjänstleverantörernas strategier för terrorisminnehåll är avgörande för att öka deras ansvarighet gentemot användarna och stärka medborgarnas förtroende för den digitala inre marknaden. Värdtjänstleverantörer som har vidtagit åtgärder eller ålagts att vidta åtgärder enligt denna förordning under ett visst kalenderår bör offentliggöra årliga transparensrapporter som innehåller information om åtgärder som vidtagits för att identifiera och avlägsna terrorisminnehåll.

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

(32) Rätten till ett effektivt rättsmedel stadfästs i artikel 19 i fördraget om Europeiska unionen (EU-fördraget) och artikel 47 i stadgan. Varje fysisk eller juridisk person har rätt till ett effektivt rättsmedel inför behörig nationell domstol mot alla åtgärder som vidtas enligt denna förordning och som kan inverka negativt på den personens rättigheter. Den rätten bör särskilt inbegripa en möjlighet för värdtjänstleverantörer och innehållsleverantörer att effektivt bestrida avlägsnandeorder eller beslut till följd av granskning av avlägsnandeorder enligt denna förordning inför domstol i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern eller fattade beslutet, och en möjlighet för värdtjänstleverantörer att effektivt bestrida ett beslut om specifika åtgärder eller sanktioner inför domstol i den medlemsstat vars behöriga myndighet fattade det beslutet.

(33) Klagomålsförfaranden utgör en nödvändig skyddsåtgärd mot att innehåll online felaktigt avlägsnas eller görs oåtkomligt när sådant innehåll är skyddat genom yttrande- och informationsfriheten. Värdtjänstleverantörer bör därför upprätta användarvänliga klagomålsmekanismer och säkerställa att klagomål hanteras snabbt och med full transparens gentemot innehållsleverantören. Kravet på att värdtjänstleverantören ska återställa innehåll som felaktigt har avlägsnats eller gjorts oåtkomligt bör inte påverka värdtjänstleverantörens möjlighet att genomdriva sina egna användarvillkor.

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

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

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

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

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

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

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

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

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

(42) Värdtjänstleverantörer bör utse eller inrätta kontaktpunkter för att underlätta snabb handläggning av avlägsnandeorder. Kontaktpunkten bör endast tjäna operativa syften. Kontaktpunkten bör bestå av någon typ av särskilda medel, interna eller externa, som möjliggör elektronisk inlämning av avlägsnandeorder och av tekniska resurser eller personalresurser som möjliggör snabb handläggning av dem. Kontaktpunkten måste inte vara belägen i unionen. Värdtjänstleverantören bör vara fri att använda en befintlig kontaktpunkt vid tillämpningen av denna förordning, under förutsättning att kontaktpunkten klarar av att fullgöra de funktioner som föreskrivs i denna förordning. I syfte att säkerställa att terrorisminnehåll avlägsnas eller görs oåtkomligt inom en timme från mottagandet av en avlägsnandeorder bör kontaktpunkten för värdtjänstleverantörer som är exponerade för terrorisminnehåll vara tillgänglig vid alla tidpunkter. Informationen om kontaktpunkten bör inbegripa information om vilket språk kontaktpunkten kan kontaktas på. För att underlätta kommunikationen mellan värdtjänstleverantörerna och de behöriga myndigheterna uppmuntras värdtjänstleverantörer att tillåta kommunikation på ett av unionsinstitutionernas officiella språk som deras användarvillkor finns tillgängliga på.

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

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

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

(46) Användningen av standardiserade mallar underlättar samarbete och informationsutbyte mellan behöriga myndigheter och värdtjänstleverantörer, och gör det möjligt för dem att kommunicera snabbare och mer effektivt. Det är särskilt viktigt att säkerställa snabba åtgärder efter mottagandet av en avlägsnandeorder. Mallar minskar översättningskostnaderna och bidrar till en högre standard för processen. Mallar för återkoppling möjliggör ett standardiserat informationsutbyte och är särskilt viktiga om värdtjänstleverantörerna inte kan följa avlägsnandeorder. Autentiserade inlämningskanaler kan garantera att avlägsnandeordern är autentisk, liksom att datum och tidpunkt för sändande och mottagande av ordern är korrekta.

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

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

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

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

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

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVSNITT I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll och tillämpningsområde

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

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

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

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

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

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

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

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

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

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

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

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

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

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

4. *erbjuda tjänster i unionen*: göra det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda de tjänster som erbjuds av en värdtjänstleverantör som har en betydande anknytning till den eller de medlemsstaterna.

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

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

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

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

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

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

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

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

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

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

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

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

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

AVSNITT II

ÅTGÄRDER MOT SPRIDNING AV TERRORISMINNEHÅLL ONLINE

Artikel 3

Avlägsnandeorder

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

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

Första stycket ska inte gälla i vederbörligen motiverade brådskande fall.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artikel 4

Förfarande för gränsöverskridande avlägsnandeorder

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

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

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

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

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

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

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

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

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

Artikel 5

Specifika åtgärder

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

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

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

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

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

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

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

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

3. Specifika åtgärder ska uppfylla samtliga följande krav:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artikel 6

Bevarande av innehåll och därtill hörande data

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

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

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

2. Det terrorisminnehåll och de därtill hörande data som avses i punkt 1 ska bevaras i sex månader från det att de avlägsnats eller gjorts oåtkomliga. Terrorisminnehållet ska på den behöriga myndighetens eller domstolens begäran bevaras under en ytterligare, specificerad period endast om och så länge som det krävs för ett sådant pågående administrativt eller rättsligt prövningsförfarande som avses i punkt 1 a.

3. Värdtjänstleverantörer ska säkerställa att terrorisminnehåll och därtill hörande data som bevaras enligt punkt 1 omfattas av lämpliga tekniska och organisatoriska skyddsåtgärder.

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

AVSNITT III

SKYDDSÅTGÄRDER OCH ANSVARIGHET

Artikel 7

Transparenskrav för värdtjänstleverantörer

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

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

3. Transparensrapporterna ska innehålla minst följande information:

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

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

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

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

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

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

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

Artikel 8

Behöriga myndigheters transparensrapporter

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

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

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

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

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

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

Artikel 9

Rättsmedel

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

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

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

Artikel 10

Klagomålsmekanismer

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

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

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

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

Artikel 11

Information till innehållsleverantörer

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

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

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

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

AVSNITT IV

BEHÖRIGA MYNDIGHETER OCH SAMARBETE

Artikel 12

Utseende av behöriga myndigheter

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

a) utfärda avlägsnandeorder enligt artikel 3,

b) granska avlägsnandeorder enligt artikel 4,

c) övervaka genomförandet av specifika åtgärder enligt artikel 5,

d) påföra sanktioner enligt artikel 18.

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

Medlemsstaterna ska säkerställa att information om kontaktpunkten offentliggörs.

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

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

Artikel 13

Behöriga myndigheter

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

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

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

Artikel 14

Samarbete mellan värdtjänstleverantörer, behöriga myndigheter och Europol

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

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

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

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

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

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

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

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

Artikel 15

Värdtjänstleverantörers kontaktpunkter

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

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

AVSNITT V

GENOMFÖRANDE OCH VERKSTÄLLIGHET

Artikel 16

Jurisdiktion

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

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

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

Artikel 17

Rättslig företrädare

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

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

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

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

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

Informationen om den rättsliga företrädaren ska offentliggöras av värdtjänstleverantören.

AVSNITT VI

SLUTBESTÄMMELSER

Artikel 18

Sanktioner

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

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

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

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

a) överträdelsens karaktär, allvar och varaktighet,

b) om överträdelsen var avsiktlig eller orsakades av vårdslöshet,

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

d) värdtjänstleverantörens finansiella styrka,

e) graden av tjänsteleverantörens samarbete med de behöriga myndigheterna,

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

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

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

Artikel 19

Tekniska krav och ändringar av bilagorna

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

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

Artikel 20

Utövande av delegeringen

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

2. Den befogenhet att anta delegerade akter som avses i artikel 19 ges till kommissionen tills vidare från och med den 7 juni 2022.

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

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

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

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

Artikel 21

Övervakning

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

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

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

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

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

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

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

Artikel 22

Genomföranderapport

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

Artikel 23

Utvärdering

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

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

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

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

Vid behov ska rapporten åtföljas av lagstiftningsförslag.

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

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

Artikel 24

Ikraftträdande och tillämpning

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

Den ska tillämpas från och med den 7 juni 2022.

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

Utfärdad i Bryssel den 29 april 2021.

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

BILAGA I

AVLÄGSNANDEORDER

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

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

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

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

AVSNITT A:

Den utfärdande behöriga myndighetens medlemsstat:

.....

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

Mottagare och, om tillämpligt, rättslig företrädare:

.....

Kontaktpunkt:

.....

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

.....

Tid och datum för utfärdande av avlägsnandeordern:

.....

Referensnummer för avlägsnandeordern:

.....

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

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

.....

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

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

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

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

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

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

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

Ytterligare information om orsakerna till att materialet anses vara terrorisminnehåll:

.....

.....

.....

AVSNITT C: Information till innehållsleverantören

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

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

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

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

Kryssa för relevant(a) ruta/rutor

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

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

AVSNITT E: Uppgifter om den utfärdande behöriga myndigheten

Typ (kryssa för relevant ruta)

☐ domare, domstol eller undersökningsdomare

☐ brottsbekämpande myndighet

☐ annan behörig myndighet → fyll även i avsnitt F

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

Den utfärdande behöriga myndighetens namn:

.....

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

.....

Dokumentnummer:

.....

Adress:

.....

Tfn (landsnummer) (riktnummer):

.....

Fax (landsnummer) (riktnummer):

.....

E-postadress .....

Datum.....

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

.....

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

AVSNITT F: Kontaktuppgifter för uppföljning

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

.....

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

.....

AVSNITT G: Information om möjligheter till prövning

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

Behörigt organ eller behörig domstol vid vilken avlägsnandeordern kan bestridas:

.....

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

.....

Länk till bestämmelser i nationell lagstiftning:

.....

BILAGA II

ÅTERKOPPLING EFTER DET ATT TERRORISMINNEHÅLL HAR AVLÄGSNATS ELLER GJORTS OÅTKOMLIGT

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

AVSNITT A:

Avlägsnandeorderns mottagare:

.....

Behörig myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för den behöriga myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för mottagaren:

.....

Tid och datum för mottagande av avlägsnandeordern:

.....

AVSNITT B: Åtgärder som vidtagits i enlighet med avlägsnandeordern

(Kryssa för relevant ruta)

☐ terrorisminnehållet har avlägsnats

☐ terrorisminnehållet har gjorts oåtkomligt i alla medlemsstater

Tid och datum då åtgärden vidtogs:

.....

AVSNITT C: Uppgifter om mottagaren

Namn på värdtjänstleverantören:

.....

ELLER

Namn på värdtjänstleverantörens rättsliga företrädare:

.....

Medlemsstat där värdtjänstleverantörens har sitt huvudsakliga verksamhetsställe:

.....

ELLER

Medlemsstat där värdtjänstleverantörens rättsliga företrädare är bosatt eller etablerad:

.....

Namn på den bemyndigade personen:

.....

Kontaktpunktens e-postadress:

.....

Datum:

.....

BILAGA III

INFORMATION OM ATT DET ÄR OMÖJLIGT ATT VERKSTÄLLA AVLÄGSNANDEORDERN

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

AVSNITT A:

Avlägsnandeorderns mottagare:

.....

Behörig myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för den behöriga myndighet som utfärdade avlägsnandeordern:

.....

Referensnummer för mottagaren:

.....

Tid och datum för mottagande av avlägsnandeordern:

.....

AVSNITT B: Utebliven verkställighet

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

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

☐ avlägsnandeordern innehåller uppenbara fel

☐ avlägsnandeordern innehåller inte tillräckligt med information

2. Redogör närmare för orsakerna till utebliven verkställighet:

.....

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

.....

AVSNITT C: Uppgifter om värdtjänstleverantören eller dess rättsliga företrädare

Namn på värdtjänstleverantören:

.....

ELLER

Namn på värdtjänstleverantörens rättsliga företrädare:

.....

Namn på den bemyndigade personen:

.....

Kontaktuppgifter (e-postadress):

.....

Underskrift:

.....

Tid och datum:

.....

Statens offentliga utredningar 2022

Kronologisk förteckning

1. Förbättrade åtgärder när barn misstänks för brott. Ju.
2. En skärpt syn på brott mot journalister och utövare av vissa samhällsnyttiga funktioner. Ju.
3. Sveriges tillgång till vaccin mot covid-19 – framgång genom samarbete och helgardering. S.
4. Minska gapet. Åtgärder för jämställda livsinkomster. A.
5. Innehållsvillkor för public service på internet – och ordningen för beslut vid förhandsprövning. Ku.
6. Hälso- och sjukvårdens beredskap – struktur för ökad förmåga. Del 1 och 2. S.
7. Kunskapsläget på kärnavfallsområdet 2022. Samhället, tekniken och etiken. M.
8. Rätt och rimligt för statligt anställda. Fi.
9. Avfallsbeskattning – En fråga om undantag? Fi.
10. Sverige under pandemin. Volym 1 Samhällets, företagens och enskildas ekonomi. Volym 2 Förutsättningar, vägval och utvärdering. S.
11. Handlingsplan för en långsiktig utveckling av tolktjänsten för döva, hörselskadade och personer med dövblindhet. S.
12. Startlån till förstagångsköpare av bostad. Fi.
13. Godstransporter på väg – vissa frågeställningar kring ett nytt miljöstyrande system. Fi.
14. Sänk tröskeln till en god bostad. Fi.
15. Sveriges globala klimatavtryck. M.
16. Ett förstärkt lagstöd för utlämnande av sekretesskyddade uppgifter till utlandet. Fö.
17. En modell för att mäta och belöna progression inom sfi. U.
18. EU:s förordning om terrorisminnehåll på internet – kompletteringar och ändringar i svensk rätt. Ju.

Statens offentliga utredningar 2022

Systematisk förteckning