Rigmor Söderberg **RR_2026_8**

Från:	Annika Götesson <annika.gotesson@regeringskansliet.se> för JU L4 <ju.l4 @regeringskansliet.se>
Skickat:	den 13 januari 2026 15:29
Till:	info; info@bris.se; registrator@bra.se; info@crd.org; domstolsverket@dom.se; huvudregistrator; info@funktionsratt.se; forvaltningsrattenistockholm; sovreby@google.com; gbg tingsratt; hovratten nedrenorrland; registrator; imy; info@internetstiftelsen.se; kansliet@sjf.se; registrator; registrator@jamstalldhetsmyndigheten.se; kammarrattenistockholm; registrator; konsumentverket; kronofogdemyndigheten@kronofogden.se; registrator; registrator@lu.se; info; registrator@mediemyndigheten.se; elvelid@meta.com; info; registrator kansli; pts; Regelrådet; justitieombudsmannen@jo.se; givarservice@rb.se; cmogensen@snapchat.com; remisser@svensktnaringsliv.se; info@advokatsamfundet.se; remiss@advokatsamfundet.se; info@sverigestidskrifter.se; sakint; sakerhetspolisen@sakerhetspolisen.se; robert.liljestrom@techsverige.se; info@teknikforetagen.se; info@tu.se; fredrik.timell@tiktok.com; registrator; tullverket; registrator
Kopia:	Åtta45 - regeringskansliet
Ämne:	[extern] Remiss av promemorian Nya möjligheter att bekämpa onlinerekrytering (Ds 2026:1) - Svar senast 13 mars 2026
Bifogade filer:	plchdr.htm; Remissmissiv.pdf
Uppföljningsflagga:	Följ upp
Flagga:	Har meddelandeflagga
Kategorier:	Rigmor
AppServerName:	public360_prod
DocumentID:	RR 2026-8:01
DocumentIsArchived:	-1

Nya möjligheter att bekämpa onlinerekrytering - Regeringen.se

OBSERVERA att de tryckta exemplaren av promemorian inte finns att beställa från tryckeriet Åtta45 förrän 20/1

Remiss av promemorian Nya möjligheter att bekämpa onlinerekrytering

Remissinstanser

1. Barnombudsmannen
2. BRIS
3. Brottsförebyggande rådet
4. Civil Rights Defenders
5. Domstolsverket
6. Ekobrottsmyndigheten
7. Funktionsrätt Sverige

8. Förvaltningsrätten i Stockholm
9. Google Sweden AB
10. Göteborgs tingsrätt
11. Hovrätten för Nedre Norrland
12. Institutet för mänskliga rättigheter
13. Integritetsskyddsmyndigheten
14. Internetstiftelsen
15. Journalistförbundet
16. Justitiekanslern
17. Jämställdhetsmyndigheten
18. Kammarrätten i Stockholm
19. Kommerskollegium
20. Konsumentverket
21. Kronofogdemyndigheten
22. Kustbevakningen
23. Lunds universitet (Juridiska fakulteten)
24. LSU – Sveriges barn och ungdomsorganisationer
25. Mediemyndigheten
26. Meta Sverige
27. Myndigheten för ungdoms- och civilsamhällesfrågor
28. Polismyndigheten
29. Post- och telestyrelsen
30. Regelrådet
31. Riksdagens ombudsmän
32. Rädda barnen
33. SnapInc
34. Svenskt näringsliv
35. Sveriges advokatsamfund
36. Sveriges Tidskrifter
37. Säkerhets- och integritetsskyddsnämnden
38. Säkerhetspolisen
39. TechSverige
40. Teknikföretagen
41. Tidningsutgivarna
42. TikTok
43. Totalförsvarets forskningsinstitut
44. Tullverket
45. Åklagarmyndigheten

Remissvaren ska ha kommit in till Justitiedepartementet **senast den 13 mars 2026**. Svaren bör lämnas per e-post till ju.remissvar@regeringskansliet.se och med kopia till Ju.L4@regeringskansliet.se. Ange diarienummer Ju2026/00046 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.
Remissvaren kommer att publiceras på regeringens webbplats.
I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i promemorian. Om remissen är begränsad till en viss del av promemorian, anges detta inom parentes efter remissinstansens namn i remisslistan. En sådan begränsning hindrar givetvis inte att remissinstansen lämnar synpunkter också på övriga delar.
Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.
För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.
Promemorian kan laddas ned från Regeringskansliets webbplats www.regeringen.se.
Remissinstanserna kan utan kostnad beställa tryckta exemplar av promemorian via ett beställningsformulär hos Åtta45.
Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Johan Stensbäck
Departementsråd

Kopia till
Åtta45, e-postadress: regeringskansliet@atta45.se

Regeringskansliet

Remiss

2026-01-13
Ju2026/00046

Justitiedepartementet
Enheten för lagstiftning om allmän ordning och säkerhet

Remiss av promemorian Nya möjligheter att bekämpa onlinerekrytering

Remissinstanser

1. Barnombudsmannen
2. BRIS
3. Brottsförebyggande rådet
4. Civil Rights Defenders
5. Domstolsverket
6. Ekobrottsmyndigheten
7. Funktionsrätt Sverige
8. Förvaltningsrätten i Stockholm
9. Google Sweden AB
10. Göteborgs tingsrätt
11. Hovrätten för Nedre Norrland
12. Institutet för mänskliga rättigheter
13. Integritetsskyddsmyndigheten
14. Internetstiftelsen
15. Journalistförbundet
16. Justitiekanslern
17. Jämställdhetsmyndigheten
18. Kammarrätten i Stockholm
19. Kommerskollegium

Telefonväxel: 08-405 10 00
Fax: 08-24 46 31
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Rosenbad
E-post: ju.registrator@regeringskansliet.se

20. Konsumentverket
21. Kronofogdemyndigheten
22. Kustbevakningen
23. Lunds universitet (Juridiska fakulteten)
24. LSU – Sveriges barn och ungdomsorganisationer
25. Mediemyndigheten
26. Meta Sverige
27. Myndigheten för ungdoms- och civilsamhällesfrågor
28. Polismyndigheten
29. Post- och telestyrelsen
30. Regelrådet
31. Riksdagens ombudsmän
32. Rädda barnen
33. SnapInc
34. Svenskt näringsliv
35. Sveriges advokatsamfund
36. Sveriges Tidskrifter
37. Säkerhets- och integritetsskyddsnämnden
38. Säkerhetspolisen
39. TechSverige
40. Teknikföretagen
41. Tidningsutgivarna
42. TikTok
43. Totalförsvarets forskningsinstitut
44. Tullverket
45. Åklagarmyndigheten

Remissvaren ska ha kommit in till Justitiedepartementet **senast den 13 mars 2026**. Svaren bör lämnas per e-post till ju.remissvar@regeringskansliet.se och med kopia till Ju.L4@regeringskansliet.se. Ange diarienummer

Ju2026/00046 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i promemorian. Om remissen är begränsad till en viss del av promemorian, anges detta inom parentes efter remissinstansens namn i remisslistan. En sådan begränsning hindrar givetvis inte att remissinstansen lämnar synpunkter också på övriga delar.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Promemorian kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av promemorian via ett beställningsformulär hos Åtta45.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Johan Stensbäck
Departementsråd

Kopia till

Åtta45, e-postadress: regeringskansliet@atta45.se

Nya möjligheter att bekämpa onlinerekrytering

Ds 2026:1

Regeringskansliet
Justitiedepartementet

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

Svara på remiss
Statsrådsberedningen, *SB PM 2021:1.*
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Omslag: Regeringskansliets standard
Tryck och remisshantering: Åtta45, Stockholm 2026

ISBN 978-91-525-1455-9 (tryck)
ISBN 978-91-525-1456-6 (pdf)
ISSN 0284-6012

Innehåll

Sammanfattning **5**

1 Författningsförslag **7**

1.1 Förslag till lag om avlägsnande av rekryteringsinnehåll online 7

1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400) 11

2 Onlinerekrytering till brott **13**

3 Rättsliga utgångspunkter **17**

3.1 Skyddet för yttrande- och informationsfrihet 17

3.2 Åtgärder mot olaglig verksamhet online 21
3.2.1 Närmare om TCO-förordningen 24
3.2.2 Närmare om förordningen om digitala tjänster 25
3.2.3 Närmare om direktivet om bekämpning av våld mot kvinnor och våld i nära relationer 27

4 Nya möjligheter att avlägsna rekryteringsinnehåll online **29**

4.1 En ny lag om avlägsnande av rekryteringsinnehåll 29

4.2 Vilket rekryteringsinnehåll ska omfattas? 31

4.3 Lagen ska endast gälla rekryteringsinnehåll som har anknytning till Sverige 42

4.4 Undantag för terrorisminnehåll 43

5 Föreläggande om avlägsnande ... 45

5.1 En möjlighet att besluta föreläggande om avlägsnande införs ... 45

5.2 Föreläggande ska utformas i enlighet med förordningen om digitala tjänster ... 49

5.3 Avlägsnande av rekryteringsinnehåll ... 52

5.4 Bevarande av rekryteringsinnehåll ... 53

6 Förhållandet till yttrande- och informationsfrihet ... 55

6.1 Den nya lagens förhållande till tryckfrihetsförordningen och yttrandefrihetsgrundlagen ... 55

7 Sanktionsavgifter ... 59

7.1 Den behöriga myndigheten ska kunna besluta om sanktionsavgift ... 59

7.2 Sanktionsavgiftens storlek ... 61

7.3 Förfarandet vid beslut om sanktionsavgift ... 63

8 Sekretess och dataskydd ... 65

8.1 Sekretess hos Polismyndigheten ... 65

8.2 Förhållandet till dataskyddsregleringen ... 69

9 Överklagande ... 75

10 Ikraftträdande- och övergångsbestämmelser ... 77

11 Konsekvenser ... 79

12 Författningskommentar ... 83

12.1 Förslaget till lag om avlägsnande av rekryteringsinnehåll online ... 83

12.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400) 93

Sammanfattning

I denna promemoria föreslås en ny lag som möjliggör för en behörig myndighet att besluta förelägganden om att innehåll online som syftar till att rekrytera personer för att begå brott (rekryteringsinnehåll) ska avlägsnas eller göras oåtkomligt. Med rekryteringsinnehåll avses innehåll som skäligen kan antas utgöra ett led i en straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet två års fängelse eller mer eller involverande av en underårig i brottslighet. Ett föreläggande om avlägsnande ska riktas mot den som tillhandahåller den plattform (värdtjänst) där innehållet finns. Innehållet ska avlägsnas eller göras oåtkomligt så snart som möjligt och senast inom en timme från mottagandet av föreläggandet. Sanktionsavgift ska kunna tas ut av en värdtjänst som överträder sina skyldigheter enligt lagen.

Förslagen syftar till att motverka onlinerekryteringen av inte minst barn och ungdomar till brottslighet och att bekämpa fenomenet crime as a service. Förslagen föreslås träda i kraft 1 september 2026.

1 Författningsförslag

1.1 Förslag till lag om avlägsnande av rekryteringsinnehåll online

Härigenom föreskrivs följande.

Lagens tillämpningsområde

1 § Denna lag reglerar förutsättningarna för att avlägsna innehåll som syftar till att rekrytera personer för att begå brott.

2 § Lagen gäller rekryteringsinnehåll som sprids till allmänheten online.

Med rekryteringsinnehåll avses innehåll som skäligen kan antas utgöra ett led i

1. straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer, eller
2. involverande av en underårig i brottslighet enligt 16 kap. 5 a § brottsbalken.

3 § Lagen gäller endast rekryteringsinnehåll som riktar sig till personer i Sverige eller avser brott som ska begås här eller mot en svensk medborgare eller någon som har hemvist i Sverige.

4 § Lagen gäller inte innehåll som omfattas av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.

Föreläggande att avlägsna rekryteringsinnehåll

5 § Den myndighet regeringen bestämmer (den behöriga myndigheten) får förelägga en värdtjänstleverantör att avlägsna rekryteringsinnehåll.

Med värdtjänstleverantör avses en sådan leverantör av värdtjänster som omfattas av Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

6 § Föreläggandet ska uppfylla de krav som följer av artikel 9.2 i förordningen om digitala tjänster.

I artikel 9 i förordningen om digitala tjänster finns bestämmelser om förfarandet efter beslut om ett sådant föreläggande.

7 § Den värdtjänstleverantör som mottar ett föreläggande ska avlägsna rekryteringsinnehållet eller göra det oåtkomligt så snart som möjligt och senast inom en timme från mottagandet av föreläggandet.

Om det är tillräckligt att innehållet görs oåtkomligt i en eller flera stater ska den behöriga myndigheten ange det i föreläggandet.

Bevarande av rekryteringsinnehåll

8 § En värdtjänstleverantör ska bevara det rekryteringsinnehåll, samt tillhörande data, som har avlägsnats eller gjorts oåtkomligt till följd av ett föreläggande.

Rekryteringsinnehållet och tillhörande data ska bevaras i sex månader från det att innehållet avlägsnats eller gjorts oåtkomligt.

Sanktionsavgifter

9 § Den behöriga myndigheten får besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som överträder någon av sina skyldigheter enligt 7 och 8 §§.

10 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 5 000 000 kronor eller, vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheten enligt 7 §, upp till ett sådant högre belopp som motsvarar fyra procent av leverantörens globala omsättning närmast föregående räkenskapsår.

Om en överträdelse som kan leda till högre sanktionsavgift än 5 000 000 kronor har skett under leverantörens första verksamhetsår eller om uppgifter om omsättningen annars saknas eller är bristfälliga, får omsättningen uppskattas.

11 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna framstår som oskäligt att ta ut avgiften.

12 § En sanktionsavgift får beslutas endast 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

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

Sanktionsavgiften tillfaller staten.

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

Överklagande

15 § Den behöriga myndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Rätt att meddela föreskrifter

16 § Regeringen eller den myndighet regeringen bestämmer får meddela ytterligare föreskrifter om informationsskyldigheten enligt artikel 9.5 i förordningen om digitala tjänster.

Denna lag träder i kraft den 1 september 2026.

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

Härigenom föreskrivs att 35 kap. 23 c § och rubriken närmast före 35 kap. 23 c § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	35 kap.
TCO-förordningen[1]	**TCO-förordningen** ***och lagen om avlägsnande av rekryterings-innehåll online***
	23 c §[2]
Sekretess gäller hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärende enligt Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och enligt lagen (2023:319) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online, *om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs*.	Sekretess gäller hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden, *om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs och uppgiften förekommer* i ärende enligt *1.* Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och enligt lagen (2023:319) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online, *eller*

[1] Senaste lydelse 2023:321.
[2] Senaste lydelse 2023:321.

2. lagen (2026:000) om avlägsnande av rekryterings-innehåll online.

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

Denna lag träder i kraft den 1 september 2026.

2 Onlinerekrytering till brott

Samhället har genomgått stora förändringar de senaste åren. Allvarlig våldsbrottslighet, framför allt skjutningar och sprängningar inom den kriminella miljön, är ett svårt problem. Den systematiska och organiserade brottsligheten har kommit att påverka allt fler delar av samhället. Angreppen riktas inte bara mot personer inom de kriminella nätverken utan även mot anhöriga. Allt oftare begås våldsbrotten utomhus och i offentliga miljöer eller riktat mot privatbostäder. Såväl offer som gärningspersoner har blivit yngre. I allt fler fall begås våldsbrotten av utförare som inte känner de tilltänkta måltavlorna. Dessa faktorer ökar risken för att utomstående drabbas, vilket också har inträffat vid åtskilliga tillfällen. Utvecklingen påverkar tryggheten i hela samhället negativt och riskerar att urholka tilltron till rättsväsendet.

Polismyndigheten bedömer i sin senaste lägesbild att cirka 17 500 personer är aktiva i kriminella nätverk. Cirka fem procent av de aktiva gängkriminella är under 18 år. Utöver de aktiva gängkriminella bedöms ytterligare cirka 50 000 personer på olika sätt ha koppling till gängkriminella. Under 2025 har antalet skjutningar som skett i landet minskat (en trend som pågått sedan 2022). Antalet sprängningar har däremot ökat. (Lägesbild över aktiva gängkriminella i Sverige, Polismyndigheten, Nationella operativa avdelningen, november 2025.)

Enligt en rapport från Brottsförebyggande rådet (Brå) observeras sedan 2013 en särskilt stor ökning av dödligt våld mot unga män (15–29 år), i linje med ökningen av dödsskjutningar i kriminell miljö. Nivån är betydligt högre i Sverige än i Europa i stort, motsvarande 42 avlidna per miljon invånare 2021 jämfört med 28 avlidna i samma grupp per miljon invånare i Europa (Dödligt våld i Sverige sedan 1990 – Omfattning, utveckling och karaktär, rapport 2024:6). En

stor del av ökningen kan kopplas till dödsskjutningar i kriminell miljö.

Den senaste utvecklingen visar att fler barn har koppling till kriminella nätverk och att de barnen blir allt yngre. Av ett flertal rapporter framgår att särskilt den allvarliga brottsligheten bland unga har ökat markant. Ytterligare en rapport från Brå visar att misstankar om vapenbrott, narkotikaöverlåtelser, utpressning och bedrägerier har ökat avsevärt under senare år bland barn som inte uppnått straffbarhetsåldern och barn under 18 år samt att unga under 21 år stod för hälften av samtliga mordmisstankar 2022. Rekryteringen till kriminella nätverk går också fortare i dag än tidigare och barn och unga begår ofta grövre brott direkt efter inträdet i ett kriminellt nätverk. Barn och unga efterfrågas av nätverken för att reducera riskerna och öka förtjänsterna för de äldre. (Barn och unga i kriminella nätverk – En studie av inträde, brott, villkor och utträde, rapport 2023:13.)

Ett fenomen, kallat crime as a service eller violence as a service, har utvecklats på senare tid. Fenomenet kännetecknas av att grova brott som sprängningar och skjutningar annonseras ut och koordineras av kriminella genom olika digitala tjänster. Det kan handla om att t.ex. transportera vapen, pengar eller narkotika, skjuta någon eller utföra en sprängning. Anstiftare och rekryterare gömmer sig bakom alias och befinner sig inte sällan utomlands. De som rekryteras och åtar sig brottsuppdragen är ofta barn och unga och saknar koppling till anstiftaren, det tänkta brottsoffret och till den plats där brottet ska utföras. Utvecklingen mot en tjänstemarknad för brott är synnerligen allvarlig. Samtidigt har de kriminella nätverken blivit allt lösare sammansatta. Utvecklingen av fenomenet har gått snabbt och Polismyndigheten bedömer att spräng- och skjutvapenvåldet som genomfördes i Sverige under 2024 och 2025 i många fall har anstiftats och koordinerats genom den digitala miljön. En liknande utveckling ses även i andra europeiska länder.

Rekryteringen av inte minst barn och unga sker alltså numera i allt högre utsträckning online och med hjälp av digitala tjänster, som har blivit centrala verktyg i de kriminella nätverkens verksamhet. Uppdragen läggs ut öppet på sociala medier, som exempelvis TikTok, Instagram och Snapchat. Brotten planeras sedan vidare i slutna grupper och krypterade chattar, i tjänster som Signal och

Telegram. Dessa tjänster gör det möjligt att kommunicera anonymt och radera meddelanden snabbt, vilket gör det svårt att upptäcka och utreda brotten. Barnen och ungdomarna uppmanas ofta att lämna information om sig själva och att ta bilder på exempelvis identitetshandlingar. Dessa kan sedan användas för att utpressa barnet eller den unga att utföra gärningen, eller för att hämnas om barnet eller den unge inte vill medverka eller misslyckas med uppdraget. Särskilt barn och unga som är sårbara med anledning av exempelvis en problematisk familjesituation, psykisk ohälsa eller kognitiva svårigheter riskerar att utnyttjas av de kriminella nätverken.

Samtidigt sprider individer och konton med kopplingar till de kriminella nätverken innehåll med bl.a. vapen och våld till följare i sociala medier och andra digitala miljöer. När barn och unga interagerar med och visar intresse för personer och ämnen kopplade till kriminalitet kan de digitala plattformarnas algoritmer leda till att de i högre grad exponeras för denna typ av innehåll.

Att kriminella nätverk rekryterar barn och unga för att begå brott utgör ett stort samhällsproblem och leder till att en ny generation av unga växer upp som en del av allvarlig brottslighet. Det är givetvis även skadligt för de enskilda som drabbas av de grova brotten, samt för deras anhöriga. Brottsoffren är inte sällan andra ungdomar. För de unga som utför brotten uppstår allvarliga negativa konsekvenser och de far ofta illa genom att pressas till fortsatt brottslighet eller riskfyllda uppdrag. Att tidigt involveras i kriminalitet kan ytterst äventyra en persons liv och hälsa. De kriminella nätverken utnyttjar alltså barn och unga på ett mycket hänsynslöst sätt. Syftet är att äldre kriminella ska undvika risker för egen del.

Det förekommer också nätbaserade grupper där förövare uppmanar och manipulerar andra att utföra och dokumentera sexuella handlingar. Filmerna sprids sedan i syfte att utpressa personerna att utföra ytterligare sexuella handlingar, plåga djur, skada sig själva eller till och med ta sina liv. Det förekommer också att de utsatta förmås att begå brott mot andra, t.ex. oprovocerade överfall. Offren är ofta minderåriga med en historik av utsatthet, psykisk ohälsa eller social isolering. Tillvägagångssättet präglas av en hög grad av sadism. För offren kan det vara svårt att bryta med grupperna. Barn och unga som deltar i sådana grupper kan både finna samhörighet inom gruppen och känna sig hotade av andra medlemmar. Genom att begå brott kan de få högre status i gruppen.

3 Rättsliga utgångspunkter

3.1 Skyddet för yttrande- och informationsfrihet

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

Europakonventionen och EU:s rättighetsstadga

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

och friheter. För åtgärder som begränsar rätten till yttrandefrihet gäller enligt både Europakonventionen och EU:s rättighetsstadga ett krav på proportionalitet. Det innebär att en avvägning ska göras mellan å ena sidan den enskildes intresse av yttrandefrihet och å andra sidan det allmänna eller enskilda intresse som motiverar begränsningen.

Regeringsformen

I 2 kap. regeringsformen (RF) finns bestämmelser om de grundläggande fri- och rättigheterna, bl.a. yttrande- och informationsfrihet. Var och en är gentemot det allmänna tillförsäkrad frihet att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor (2 kap. 1 § första stycket 1). Var och en är också tillförsäkrad informationsfrihet, dvs. friheten att inhämta och ta emot upplysningar samt att i övrigt ta del av andras yttranden (2 kap. 1 § första stycket 2).

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

Yttrande- och informationsfriheten enligt regeringsformen är inte absolut utan kan begränsas genom lag under vissa förutsättningar (2 kap. 20 § första stycket 1). En begränsning får endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på

grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 §). Liksom enligt Europakonventionen och EU:s rättighetsstadga gäller alltså även enligt regeringsformen ett krav på proportionalitet vid inskränkningar av yttrande- och informationsfriheten. Utöver dessa grundläggande krav gäller att yttrande- och informationsfriheten enbart får begränsas med hänsyn till rikets säkerhet, folkförsörjningen, allmän ordning och säkerhet, enskildas anseende, privatlivets helgd eller förebyggandet och beivrandet av brott, eller i övrigt om särskilt viktiga skäl föranleder det (2 kap. 23 § första stycket). När lagstiftaren överväger en begränsning ska vikten av vidaste möjliga yttrande- och informationsfrihet i politiska, religiösa, fackliga, vetenskapliga och kulturella angelägenheter särskilt beaktas (2 kap. 23 § andra stycket).

Tryckfrihetsförordningen

Den särskilda grundlagsregleringen i tryckfrihetsförordningen omfattar skrifter som framställs i tryckpress och, om vissa förutsättningar är uppfyllda, skrifter som har mångfaldigats genom fotokopiering eller liknande teknik (1 kap. 2 §). Inom lagens tillämpningsområde gäller både ett censurförbud och den s.k. exklusivitetsprincipen, som innebär att ingripanden på grund av missbruk av tryckfriheten endast får göras i de fall som anges i tryckfrihetsförordningen (1 kap. 8 och 9 §§).

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

Yttrandefrihetsgrundlagen

Den särskilda grundlagsregleringen i yttrandefrihetsgrundlagen är i huvudsak tillämplig på två olika kommunikationstekniker. Den

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

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

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

3.2 Åtgärder mot olaglig verksamhet online

På senare år har det skett ett omfattande arbete inom EU för att motverka olaglig och skadlig verksamhet på internet. Bland annat har det antagits ett flertal rättsakter som innehåller bestämmelser om avlägsnande av olagligt innehåll online.

Ett exempel på en sådan rättsakt är Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online (här kallad TCO-förordningen) som tillämpas sedan den 7 juni 2022. Förordningen ger nationella behöriga myndigheter, i Sverige Polismyndigheten, befogenhet att utfärda en order om att en s.k. värdtjänstleverantör ska avlägsna terrorisminnehåll från sin värdtjänst. Polismyndigheten har inrättat en särskild enhet, Internet Referral Unit (IRU) som ansvarar för att utfärda sådana ordrar. IRU ansvarar även för de frivilliga mekanismer som finns för att anmäla olagligt innehåll online till värdtjänstleverantörer.

Bestämmelser om åtgärder för att ta bort visst onlinematerial finns också i Europaparlamentets och rådets direktiv (EU) 2024/1385 av den 14 maj 2024 om bekämpning av våld mot kvinnor och våld i nära relationer. En utredning om genomförande av direktivet i svensk rätt pågår för närvarande (Ju 2025:07).

En central rättsakt när det gäller att motverka skadlig verksamhet på internet är Europaparlamentets och rådets förordning (EU) 2022/2065 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster). Förordningen innehåller inte några regler om att medlemsstaterna får besluta föreläggande om att avlägsna olagligt innehåll. Däremot reglerar förordningen medlemsstaternas skyldighet att säkerställa att föreläggande utformas och hanteras i enlighet med vissa krav. Den rättsliga grunden för att besluta föreläggande ska finnas i annan unionsrätt eller i nationell rätt. Förordningen innehåller också särskilda bestämmelser om skydd av minderåriga online. Bland annat ska leverantörer av onlineplattformar som är tillgängliga för minderåriga på sina tjänster införa lämpliga och proportionerliga åtgärder för att säkerställa en hög nivå av integritet, säkerhet och trygghet för minderåriga. Kommissionen har också tagit fram riktlinjer i syfte att hjälpa onlineplattformar att skapa en rättvisare och säkrare onlineupplevelse för barn och tonåringar i EU.

I sammanhanget kan också nämnas att det pågår förhandlingar om en EU-förordning som är tänkt att ersätta Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet. Den nu gällande förordningen upphör att gälla i april 2026. Syftet med förslaget till en ny förordning är att upprätta en tydlig och harmoniserad rättslig ram för att förebygga och bekämpa sexuella övergrepp mot barn på nätet. Förslaget innehåller bl.a. bestämmelser om utfärdande av avlägsnandeordrar beträffande material med sexuella övergrepp mot barn.

Sverige har också skrivit under den s.k. Jutland-deklarationen, en EU-deklaration om skydd av barn och unga online. Deklarationen syftar till att stärka arbetet med att skapa en tryggare och mer åldersanpassad digital värld för EU:s barn och unga. I deklarationen lyfts behovet av en effektiv implementering av EU:s digitala regelverk såsom förordningen om digitala tjänster och AI-förordningen. För att säkerställa att plattformar vidtar proportionerliga skyddsåtgärder för minderåriga betonas i deklarationen även ett starkt samarbete mellan medlemsländerna och kommissionen.

När det gäller åtgärder på nationell nivå har regeringen tagit fram en nationell strategi mot organiserad brottslighet. Den innehåller prioriteringar, åtgärder och mål för att öka samhällets motståndskraft mot den organiserade brottsligheten. Fem mål ska vara vägledande i arbetet: stoppa kriminella karriärer, minska tillgången på illegala vapen och explosiva varor, slå sönder den kriminella ekonomin, bygga robusthet mot otillåten och otillbörlig påverkan samt säkerställa tillförlitliga identiteter och en effektiv informationsförsörjning. I målet att stoppa kriminella karriärer ingår att motverka att unga socialiseras och rekryteras in i kriminalitet (skr. 2023/24:67). Regeringen har även beslutat skrivelsen Barriärer mot brott – en socialpreventiv strategi mot kriminella nätverk och annan brottslighet (skr. 2023/24:68). I fokus för strategin står sociala brottsförebyggande insatser för att bl.a. motverka att barn och unga involveras i kriminella nätverk och annan brottslighet samt att få individer som begår brott att lämna kriminaliteten bakom sig. Vidare

kan nämnas att regeringen i januari 2025 gav Brå i uppdrag att öka kunskapen om hur kriminella nätverk rekryterar barn och unga i sociala medier och andra digitala miljöer för att begå brott (Ju2025/00155). Samtidigt gav regeringen Totalförsvarets forskningsinstitut (FOI) i uppdrag att öka kunskapen om hur en kriminell livsstil marknadsförs i sociala medier och andra digitala miljöer samt hur detta kan påverka barns och ungas attityder till våld och kriminalitet (Ju2025/00157). Myndigheterna ska också föreslå åtgärder som motverkar denna problematik. Uppdragen ska redovisas senast oktober 2026. Redovisningarna kommer att utgöra ett viktigt bidrag för att höja den allmänna kunskapsnivån och för att förbättra samarbetet mellan myndigheter och plattformar. Dessutom har regeringen nyligen tillsatt en utredning för att bl.a. analysera förutsättningarna för att införa en åldersgräns för barns användning av sociala medier. Syftet är att stärka skyddet för barns hälsa och trygghet i digitala miljöer (dir. 2025:91).

Sedan 1998 gäller lagen (1998:112) om ansvar för elektroniska anslagstavlor (här kallad BBS-lagen). BBS-lagen är tillämplig på elektroniska anslagstavlor, dvs. tjänster för elektronisk förmedling av meddelanden. Meddelanden i lagens mening kan vara text, bild, ljud eller information i övrigt (1 §). Den som tillhandahåller en sådan tjänst har enligt BBS-lagen bl.a. en skyldighet att ha viss uppsikt över tjänsten (4 §) och att ta bort meddelanden från tjänsten, eller på annat sätt förhindra vidare spridning av dessa, om meddelandets innehåll uppenbart är sådant som avses i vissa angivna brottsbestämmelser (5 § första stycket 1). Skyldigheten enligt 4 § att ha viss uppsikt över tjänsten gäller inte för den som tillhandahåller en elektronisk anslagstavla som är en förmedlingstjänst enligt förordningen om digitala tjänster (4 a §). För den som tillhandahåller en förmedlingstjänst gäller skyldigheten enligt 5 § första stycket när det kommit till tillhandahållarens kännedom att meddelandet finns på tjänsten. Den tjänstetillhandahållare som uppsåtligen eller av grov oaktsamhet bryter mot skyldigheten enligt 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 skall inte dömas till ansvar (7 § första stycket). BBS-lagen gäller inte meddelanden som omfattas av TCO-förordningen (2 § 5).

3.2.1 Närmare om TCO-förordningen

TCO-förordningen innehåller regler för att åtgärda missbruk av värdtjänster för spridning av terrorisminnehåll online till allmänheten (artikel 1.1). Förordningen ger de nationella behöriga myndigheterna vissa befogenheter och ålägger värdtjänstleverantörer vissa skyldigheter. Förordningen kompletteras av lagen (2023:319) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online (här kallad TCO-lagen).

TCO-förordningen är tillämplig på värdtjänstleverantörer som erbjuder tjänster i EU, oberoende av deras huvudsakliga verksamhetsställe, i den mån de sprider information till allmänheten (artikel 1.2). Begreppet värdtjänstleverantör definieras, delvis genom en hänvisning, som en leverantör av någon av alla informationssamhällets tjänster som består i att information som tillhandahållits av en innehållsleverantör lagras på dennes begäran (artikel 2.1). Med informationssamhällets tjänster avses tjänster som vanligtvis utförs mot ersättning (dvs. kommersiella tjänster) på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I skälen till förordningen utvecklas begreppet något: Förordningen bör tillämpas på sådana leverantörer av 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 är av rent teknisk, automatisk och passiv karaktär. Begreppet lagring bör förstås som förvaring av data i minnet hos en fysisk eller virtuell server (skäl 13). Det innebär att förordningen exempelvis bör omfatta leverantörer av sociala medietjänster, video-, bild- och 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 14).

En värdtjänstleverantör behöver inte ha sitt huvudsakliga verksamhetsställe i unionen för att förordningen ska vara tillämplig, utan det är tillräckligt att leverantören erbjuder tjänster i unionen. Med detta avses att göra det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda de tjänster som erbjuds av en värdtjänstleverantör som har en betydande anknytning

till den eller de medlemsstaterna (artikel 2.4). Betydande anknytning innebär i sin tur att en värdtjänstleverantör har en anknytning till en eller flera medlemsstater som följer antingen av dennes verksamhetsställe i unionen eller av särskilda faktiska kriterier. Dessa kriterier kan vara att värdtjänstleverantören har ett betydande antal användare av dess tjänster i en eller flera medlemsstater eller att verksamheten är riktad mot en eller flera medlemsstater (artikel 2.5). En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen ska skriftligen utse en fysisk eller juridisk person till sin rättsliga företrädare i unionen (artikel 17.1)

För att förordningen ska vara tillämplig krävs att det är fråga om spridning till allmänheten (artikel 1). Med begreppet spridning till allmänheten avses tillgängliggörande av information på begäran av en innehållsleverantör för ett potentiellt obegränsat antal personer (artikel 2.3).

Varje medlemsstat ska utse en eller flera s.k. behöriga myndigheter som förses med ett antal befogenheter enligt förordningen. Den behöriga myndigheten kan bl.a. utfärda och granska avlägsnandeordrar, övervaka genomförandet av specifika åtgärder och påföra sanktioner (artikel 12.1). En avlägsnandeorder innebär en skyldighet för en värdtjänstleverantör att avlägsna terrorisminnehåll eller göra det oåtkomligt i samtliga medlemsstater. Detta ska ske så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern (artikel 3). Regeringen har utsett Polismyndigheten till svensk behörig myndighet.

TCO-förordningen hindrar inte medlemsstaterna från att vidta frivilliga åtgärder (skäl 40). En behörig myndighet kan alltså, innan åtgärder enligt förordningen vidtas, via en mer informell kontakt uppmärksamma en värdtjänstleverantör på visst innehåll. Sådana kontakter får endast ske inom de ramar som tryck- och yttrandefriheten tillåter och på ett sådant sätt att åtgärden inte uppfattas som tvingande av värdtjänstleverantören.

3.2.2 Närmare om förordningen om digitala tjänster

Förordningen om digitala tjänster trädde i kraft den 16 november 2022 och tillämpas i sin helhet sedan den 17 februari 2024.

Genom förordningen fastställs enhetliga regler för s.k. leverantörer av förmedlingstjänster. Förordningen är tillämplig på förmedlingstjänster som erbjuds till tjänstemottagare som har sitt etableringsställe eller befinner sig i unionen, oavsett var de leverantörer som tillhandahåller dessa förmedlingstjänster har sitt etableringsställe (artikel 2). Tjänstemottagare definieras som en fysisk eller juridisk person som använder en förmedlingstjänst, i synnerhet för att söka information eller göra den tillgänglig (artikel 3).

De förmedlingstjänster som omfattas av förordningen definieras i artikel 3. De är uppdelade i kategorierna enbart vidarefordran, cachning, värdtjänster (varav vissa är onlineplattformar av olika storlek) samt mycket stora onlinesökmotorer. Förmedlingstjänster kan exempelvis utgöra en infrastruktur för tredje parts innehåll, vara eller tjänst, t.ex. ett meddelande, en uppladdad video, ett blogginlägg eller en vara som bjuds ut till försäljning (prop. 2023/24:160 s. 19).

En värdtjänst definieras i förordningen som en tjänst som består av lagring av information som tillhandahålls av en tjänstemottagare och som sker på dennes begäran. Förordningen innehåller vidare en särskild definition av onlineplattformar. Med onlineplattform avses en värdtjänst som på begäran av en tjänstemottagare lagrar och sprider information till allmänheten, såvida inte denna verksamhet enbart utgör en extrafunktion av mindre betydelse inom en annan tjänst eller en funktion av mindre betydelse inom den huvudsakliga tjänsten och om denna extrafunktion eller funktion av objektiva och tekniska skäl inte kan användas utan denna andra tjänst, och integreringen av extrafunktionen eller funktionen inte är ett sätt att kringgå tillämpningen av bestämmelserna i förordningen. Med spridning till allmänheten avses att på begäran av den tjänstemottagare som tillhandahållit informationen göra den tillgänglig för ett potentiellt obegränsat antal tredje parter.

Genom förordningen infördes bl.a. en skyldighet för leverantörer av förmedlingstjänster att införa mekanismer för anmälan av förekomst av olagliga varor och tjänster eller annat olagligt innehåll och regler för skydd av minderåriga online (artikel 16 och 28). Förordningen innehåller också en skyldighet för leverantör av värdtjänster att underrätta brottsbekämpande eller rättsliga myndigheter om de får kännedom om information som ger upphov till misstanke om att ett brott som inbegriper ett hot mot en eller

flera människors liv eller säkerhet har skett, håller på att ske eller sannolikt kommer att ske (artikel 18).

Förordningen ger inte i sig rättslig grund för nationella behöriga myndigheter att förelägga en leverantör att ta bort olagligt innehåll. Bestämmelser om vad som utgör olagligt innehåll och rätten att förelägga leverantörer av förmedlingstjänster att vidta åtgärder mot sådant innehåll eller att tillhandahålla viss specifik information ska finnas i annan unionsrätt eller i nationell rätt. Förordningens bestämmelser om föreläggande att agera mot olagligt innehåll (artikel 9) och att tillhandahålla information (artikel 10) reglerar medlemsstaternas skyldighet att säkerställa att föreläggandena utformas i enlighet med vissa krav och att beslutade föreläggande hanteras och följs upp på visst sätt. Enligt skälen till förordningen bör berörda nationella myndigheter kunna utfärda föreläggande mot innehåll som anses olagligt på grundval av unionsrätten eller nationell rätt i överensstämmelse med unionsrätten, i synnerhet stadgan, och att rikta dem till leverantörer av förmedlingstjänster, även sådana som är etablerade i en annan medlemsstat (skäl 34).

3.2.3 Närmare om direktivet om bekämpning av våld mot kvinnor och våld i nära relationer

Direktivet om bekämpning av våld mot kvinnor och våld i nära relationer utgör den första EU-lagstiftningen om bekämpning av våld mot kvinnor. Syftet med direktivet är att fastställa en heltäckande ram för att effektivt bekämpa våld mot kvinnor och våld i nära relationer inom EU. Direktivet ställer bl.a. krav på att alla medlemsstater kriminaliserar kvinnlig könsstympning, tvångsäktenskap och brott på nätet såsom nättrakasserier och delning av intima eller manipulerade bilder utan samtycke och offentlig uppmaning till våld eller hat på nätet (artikel 3–8). Brotten ska vara belagda med effektiva, proportionerliga och avskräckande straffrättsliga påföljder (artikel 10). Direktivet ålägger också medlemsstaterna att vidta lämpliga åtgärder för att förebygga våld mot kvinnor och våld i nära relationer och fastställer standarder för skydd och stöd till brottsoffer. Som framgår ovan har regeringen gett en utredare i uppdrag att överväga vilka åtgärder som krävs i svensk rätt för att genomföra direktivet.

Artikel 23 i direktivet innehåller bestämmelser om åtgärder för att avlägsna visst onlinematerial. Enligt artikeln ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att visst material som är allmänt tillgängligt online skyndsamt avlägsnas eller görs oåtkomligt. Det handlar om material som 1) visar handlingar med uttrycklig sexuell innebörd eller en persons intima kroppsdelar eller manipulerat sådant material som gjorts tillgängligt för allmänheten utan personens samtycke och 2) utgör vissa former av nättrakasserier eller uppmaning till våld eller hat mot en grupp personer eller en medlem av en grupp, utpekad med åberopande av kön. De åtgärder som medlemsstaterna ska vidta ska innefatta en möjlighet för behöriga myndigheter att utfärda bindande rättsliga föreläggande att avlägsna sådant material eller göra det oåtkomligt. Sådana föreläggande ska åtminstone uppfylla de villkor som anges i artikel 9.2 i förordningen om digitala tjänster. Föreläggande ska riktas till värdtjänstleverantörer. Om avlägsnande inte är möjligt får de behöriga myndigheterna även rikta föreläggande att göra det berörda materialet oåtkomlig till andra relevanta leverantörer av förmedlingstjänster än värdtjänstleverantörer vilka har teknisk och operativ kapacitet att vidta åtgärder i fråga om det berörda materialet.

4 Nya möjligheter att avlägsna rekryteringsinnehåll online

4.1 En ny lag om avlägsnande av rekryteringsinnehåll

Förslag

Det ska införas en lag om avlägsnande av rekryteringsinnehåll. Lagen ska reglera förutsättningarna för att avlägsna innehåll online som syftar till att rekrytera personer för att begå brott.

Bedömning

Lagen bör utformas på liknande sätt som lagstiftningen om åtgärder mot spridning av terrorisminnehåll online.

Skälen för förslaget och bedömningen

Den utbredda grova brottsligheten och barn och ungas involvering i denna är ett stort samhällsproblem. För att långsiktigt komma till rätta med detta behöver rekryteringen till kriminella nätverk bekämpas. Det gäller inte minst rekryteringen av barn och unga.

De digitala plattformarna som används för rekryteringen har själva störst möjlighet att stoppa rekryteringsannonser för kriminalitet i sina respektive system. Brottsbekämpande myndigheter kan dock bidra genom att arbeta i de digitala miljöerna, samarbeta med plattformarna och anmäla det olagliga innehåll som de upptäcker. Polismyndigheten arbetar exempelvis aktivt med s.k.

referrals, genom vilka polisen kan uppmärksamma en värdtjänstleverantör på att det finns innehåll på plattformen som kan utgöra brott. Det är i dessa fall värdtjänstleverantören själv som beslutar om innehållet ska tas bort eller inte och då oftast med utgångspunkt i leverantörens användarvillkor. Polismyndigheten har initierat möten med representanter från de stora sociala medie- och spelplattformarna för att fördjupa samarbetet och öka kunskapen om hur plattformarna används för att rekrytera utförare och koordinera brott. Polismyndigheten arbetar också med s.k. digital patrullering eller nätpatrullering, på exempelvis sociala medier och spelplattformar. På detta sätt kan myndigheten upptäcka bl.a. grooming, hatbrott, digital utpressning och rekrytering av barn till kriminalitet. Sverige har också tillsammans med de övriga nordiska länderna fört fram politiska krav på större ansvar från företagen som äger de plattformar som används. Arbetet har fortsatt på EU-nivån i samarbete med bl.a. kommissionen, som tar upp frågan i strategin för EU:s inre säkerhet från april 2025. Inom Europol leder svensk polis ett operativt samarbete med målet att tillsammans med rättsvårdande myndigheter från ett antal andra länder angripa crime as a service och den digitala rekryteringen av ungdomar till grov våldsbrottslighet. I insatsen, som inleddes 2025, ingår underrättelseutbyte, gemensamma utredningar och kartläggningar, åtgärder mot kriminella tjänsteleverantörer och samarbete med techbolag.

Ovan nämnda åtgärder är viktiga i kampen för att motverka onlinerekryteringen till brott. De mekanismer som finns fungerar i vissa fall bra, men kan med hänsyn till det allvarliga läget inte anses tillräckliga. När det gäller terrorisminnehåll online har Polismyndigheten möjlighet att med stöd av TCO-förordningen utfärda avlägsnandeordrar som innebär att de tjänster där materialet finns ska avlägsna materialet eller göra det oåtkomligt så snart som möjligt. Förordningen gäller bara terrorisminnehåll och kan alltså inte användas avseende annat olagligt innehåll. Inte heller förordningen om digitala tjänster ger rättslig grund för att besluta föreläggande om att avlägsna olagligt innehåll online. Däremot förutsätter förordningen att sådana föreläggande ska kunna beslutas med stöd i annan unionsrätt eller nationell rätt. Förordningen innehåller bestämmelser om bl.a. utformningen och hanteringen av sådana föreläggande. Enligt skälen till förordningen ska berörda nationella myndigheter kunna utfärda föreläggande

mot innehåll som är olagligt enligt unionsrätten eller nationell rätt och rikta dem till leverantörer av förmedlingstjänster, även sådana som är etablerade i en annan medlemsstat (skäl 34).

För att motverka onlinerekryteringen och utvecklingen med crime as a service bör det vara möjligt att vidta handlingsdirigerande åtgärder för att få bort de kriminella rekryteringsannonserna från internet. Den ordning som finns för att avlägsna terrorisminnehåll fungerar i allt väsentligt bra och det framstår därför som ändamålsenligt att införa motsvarande befogenheter för att komma åt onlinerekryteringen, dvs. att en myndighet ges befogenhet att besluta förelägganden om att visst innehåll ska tas bort eller göras oåtkomligt. En ny lag med bestämmelser om avlägsnande av rekryteringsinnehåll bör därför införas. Den nya lagens innehåll bör som utgångspunkt utformas på liknande sätt som TCO-förordningen och TCO-lagen.

Rekrytering till kriminalitet som sker på annat sätt än via internet omfattas inte av förslagen i denna promemoria. Att möjliggöra att innehåll som publicerats online kan avlägsnas genom myndighetsåtgärder innebär ett ingrepp i yttrande- och informationsfriheten. Sådana ingrepp får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett dem. Vilket innehåll som ska omfattas och hur lagen i övrigt ska avgränsas behandlas nedan.

4.2 Vilket rekryteringsinnehåll ska omfattas?

Förslag

Lagen ska gälla rekryteringsinnehåll som sprids till allmänheten online.

Med rekryteringsinnehåll ska avses innehåll som skäligen kan antas utgöra ett led i

1. straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer, eller
2. involverande av en underårig i brottslighet enligt 16 kap. 5 a § brottsbalken.

Skälen för förslaget

Den nya lagen bör omfatta rekryteringsinnehåll som sprids till allmänheten

Som framgår ovan är syftet med den föreslagna lagen att komma åt rekryteringen online av bl.a. barn och unga till kriminalitet. I detta avsnitt behandlas vilken typ av innehåll som lagen bör träffa.

Enligt TCO-förordningen har den behöriga myndigheten i varje medlemsstat befogenhet att utfärda en avlägsnandeorder med krav på att värdtjänstleverantörer ska avlägsna terrorisminnehåll eller göra det oåtkomligt (artikel 3). Förordningen är endast tillämplig på värdtjänstleverantörer i den mån de sprider information till allmänheten (artikel 1.2). Även tillämpningsområdet för förordningen om digitala tjänster är när det gäller sådana värdtjänster som är onlineplattformar begränsat till plattformar som sprider information till allmänheten (artikel 2.1 och 3 i). Med begreppet spridning till allmänheten avses i förordningen om digitala tjänster att på begäran av den tjänstemottagare som tillhandahållit informationen göra den tillgänglig för ett potentiellt obegränsat antal tredje parter (artikel 3 k).

Ett föreläggande att avlägsna innehåll enligt den nya lagen kommer att utgöra ett sådant föreläggande som avses i artikel 9 i förordningen om digitala tjänster. För att bli kunna bli föremål för ett avlägsnande ska innehållet alltså ha spridits på en sådan värdtjänst som omfattas av förordningen, t.ex. en sådan onlineplattform som sprider innehåll till allmänheten. Den nya lagen bör också som utgångspunkt utformas på liknande sätt som TCO-förordningen och TCO-lagen. Det bör därför framgå av den nya lagen att den är tillämplig på innehåll som sprids till allmänheten.

Kravet på spridning till allmänheten i den nya lagen bör innebära att innehållet görs tillgängligt för ett potentiellt obegränsat antal personer, oberoende av om dessa personer verkligen tar del av informationen (jfr artikel 3 k förordningen om digitala tjänster). De kriminella rekryteringsannonserna läggs ofta ut öppet i sociala medier. Det förekommer också att annonseringen sker i chattgrupper som kan bestå av flera tusen användare. För att ta del av sådant innehåll krävs ofta dels ett eget konto på plattformen, dels att den som administrerar kontot eller chattgruppen godkänner en följarförfrågan eller en begäran om att få delta i chatten. För att

hindra rekryteringen behöver sådant innehåll omfattas av lagstiftningen. Mot den bakgrunden bör även sådant innehåll som endast är åtkomligt för personer som t.ex. har ett konto på en viss social medieplattform eller liknande anses spritt till allmänheten, förutsatt att det i princip är möjligt för var och en att registrera ett sådant konto. Detsamma bör gälla innehåll som sprids i t.ex. en chattgrupp. Innehåll som delas t.ex. i privata chattar mellan enskilda individer och i e-postmeddelanden faller däremot utanför tillämpningsområdet för lagen. I och med att lagen inte kommer att omfatta rent privata meddelanden minskar risken för oproportionerliga ingrepp i enskildas fri- och rättigheter.

Nästa fråga att överväga är om lagstiftningen bör avgränsas så att den enbart ska träffa rekryteringen av barn och unga. De aktuella sociala medierna och chattgrupperna är dock ofta sådana som både barn och vuxna har åtkomst till. Det är i regel svårt att bedöma åldern på mottagarna av innehållet. Det skulle motverka lagstiftningens syfte om innehåll skulle kunna tas bort först efter att det gjorts en bedömning av att det syftar till att rekrytera just barn eller unga. Slutligen är det också av stor vikt att den allvarliga utvecklingen med crime as a service kan stävjas oavsett om det är barn eller vuxna som åtar sig att utföra de brottsliga uppdragen. Någon sådan avgränsning bör därför inte göras.

Förutom att barn och unga rekryteras till att utföra t.ex. grova våldsbrott förekommer det att de på annat sätt utpressas och manipuleras online. Det kan handla om nätbaserade grupper där förövare pressar barn och unga till att t.ex. utföra sexuella handlingar, skada sig själva eller till och med ta sina liv. Det förekommer också att barn och unga pressas till att begå brott mot andra, t.ex. oprovocerade överfall. Detta är en mycket allvarlig utveckling som måste motverkas. I dessa fall är det dock, till skillnad från onlinerekryteringen, oftast inte fråga om innehåll som läggs ut öppet på sociala medier och andra digitala plattformar. Det rör sig i stället huvudsakligen om manipulationer och påtryckningar som sker i privata chattar mellan enskilda individer, dvs material som polisen normalt inte kan få åtkomst till annat än genom hemliga tvångsmedel. Det är därför i regel inte möjligt att få bort sådant innehåll genom föreläggande om avlägsnande. Detta fenomen behöver i stället angripas genom andra utredningsåtgärder där fokus ligger på att identifiera förövare och offer snarare än att ta bort

innehållet från internet. Skulle sådant innehåll spridas till allmänheten, dvs. publiceras t.ex. på sociala medier eller i en öppen chattgrupp, kan det dock omfattas av den nya lagen om syftet är att förmå barnet eller den unge att begå ett brott (se vidare nedan).

Regleringen bör träffa innehåll som utgör ett led i en straffbar förberedelse eller stämpling till vissa brott

Som framgår ovan ska lagen gälla innehåll som syftar till att rekrytera någon för att begå brott. För att lagstiftningen ska vara proportionerlig och förenlig med grundläggande fri- och rättigheter behöver den utformas på ett sådant sätt att den endast träffar sådant innehåll som i sig kan vara brottsligt. Innehållet måste alltså avse en rekrytering som i sig kan vara straffbar.

Att rekrytera eller försöka rekrytera någon för att utföra ett brott kan vara straffbart som stämpling eller anstiftan till brott. Med stämpling förstås att någon i samråd med någon annan beslutar gärningen eller att någon söker anstifta någon annan eller åtar eller erbjuder sig att utföra gärningen (23 kap. 2 § andra stycket brottsbalken). Straffet för stämpling ska bestämmas under den högsta och får sättas under den lägsta gräns som gäller för fullbordat brott. Högre straff än fängelse i två år får bestämmas endast om fängelse i sex år eller mer kan följa på det fullbordade brottet. Om faran för att brottet skulle fullbordas var ringa eller om gärningen med hänsyn till andra omständigheter är mindre allvarlig, ska det inte dömas till ansvar. Stämpling till brott som innebär fara för annans liv, hälsa eller personliga säkerhet kan inte anses som mindre allvarligt (prop. 2015/16:113 s. 96).

För anstiftan döms den som förmått någon annan att utföra ett brott (23 kap. 4 § brottsbalken). För straffansvar krävs att den anstiftade inte hade utfört gärningen utan anstiftarens agerande. Det krävs också, till skillnad från stämpling, att en straffbelagd gärning har utförts av den anstiftade. Det är tillräckligt att det kommit till stånd ett straffbart försök eller en straffbar förberedelse eller stämpling.

Ansvar för anstiftan och stämpling till brott är straffbart även i de fall då den som anstiftats att utföra gärningen är under 15 år och alltså inte själv kan dömas till ansvar för brott.

Regeringen har i propositionen Ett utvidgat straffansvar för försök, förberedelse och stämpling till brott (prop. 2025/26:49) föreslagit vissa ändringar i 23 kap. 2 § brottsbalken. Bland annat föreslås att det ska vara straffbart som förberedelse att utlova betalningsmedel som betalning för ett brott eller för att täcka kostnader för utförandet av ett brott. I propositionen föreslås också att det ska införas ett undantag när det gäller det s.k. farerekvisitet i 23 kap. 2 § brottsbalken. Undantaget gäller situationer då faran för brottets fullbordan var ringa eller utesluten till följd av en myndighets åtgärd för att bekämpa brott. I dessa fall ska det ändå dömas till ansvar för förberedelse eller stämpling till brott. Som exempel nämns situationer när polisen ingriper vid förberedelse eller stämpling till brott på digitala plattformar för att förhindra att någon åtar sig att utföra ett allvarligt våldsbrott (s. 56).

De rekryteringsannonser som publiceras online kan många gånger till sitt innehåll vara sådant att det uppfyller kraven för att utgöra ett led i en straffbar stämpling eller anstiftan till brott. I de flesta fall kommer det inte att vara möjligt att avgöra om det är fråga om stämpling eller anstiftan eftersom man kommer sakna kännedom om huruvida något brott med anledning av innehållet har utförts. Eftersom stämpling till brott utgör ett försök att anstifta någon kommer det dock i praktiken att sakna betydelse för tillämpningen av den nya lagen.

Om lagstiftningen avgränsas till att gälla innehåll som utgör ett led i stämpling, anstiftan eller förberedelse till brott kommer den alltså endast att träffa rekryteringsinnehåll som i sig är brottsligt. Frågan är dock om en sådan avgränsning är tillräcklig eller om det krävs någon ytterligare begränsning för att lagstiftningen ska vara proportionerlig. Som framgår ovan är syftet med den nya lagen att komma åt utvecklingen med en ökad rekrytering online av inte minst barn och unga till kriminalitet och att angripa utvecklingen av crime as a service. Detta intresse väger mycket tungt. Samtidigt finns det flera viktiga motstående intressen som måste beaktas vid utformningen av regleringen – inte minst friheten att uttrycka sina åsikter och informationsfriheten. Anstiftan är straffbart beträffande alla brott enligt brottsbalken och för brott enligt specialstraffrätten om fängelse är föreskrivet för brottet. Det innebär att anstiftan är straffbart även vid bötesbrott och andra mindre allvarliga brott. Även förberedelse till brott är i vissa fall straffbart för bötesbrott.

Att låta allt innehåll som kan utgöra ett led i anstiftan eller förberedelse till brott skulle mot den bakgrunden inte vara proportionerligt.

För att uppfylla kraven på proportionalitet bör regleringen avgränsas till innehåll som syftar till att rekrytera personer till mer allvarlig brottslighet. Som utgångspunkt behöver lagen utformas så att den träffar sådan allvarlig brottslighet som är vanligt förekommande vid onlinerekrytering. Det gäller inte minst skjutningar och sprängningar. Även annan brottslighet som är vanligt förekommande vid rekrytering online bör dock omfattas, exempelvis andra grova våldsbrott än mord, grova vapenbrott, narkotikabrott och penningtvättsbrott.

Ett sätt att åstadkomma en avgränsning är att införa en brottskatalog. Utvecklingen med onlinerekrytering går dock snabbt och det är svårt att med tillräcklig grad av precision peka ut vilka brott som bör omfattas av en sådan katalog. Det är också viktigt att lagstiftningen kommer att kunna tillämpas mot onlinerekryteringen över tid. En lösning med en brottskatalog är inte tillräckligt flexibel och bör därför inte väljas. Ett annat sätt att avgränsa omfattningen är att ange att lagen gäller rekrytering till brott av visst slag. t.ex. ”allvarliga brott mot liv, hälsa eller säkerhet”. En sådan avgränsning skulle innebära att bl.a. allvarlig våldsbrottslighet, såsom mord och grov misshandel omfattas. Dessutom skulle annan allvarlig brottslighet mot människors liv eller säkerhet, såsom allmänfarlig ödeläggelse och mordbrand, omfattas. Samtidigt skulle flera andra brott som det är angeläget att lagstiftningen träffar, som exempelvis narkotikabrott, falla utanför. Det framstår därför inte som lämpligt att avgränsa lagen till ”allvarliga brott mot liv, hälsa eller säkerhet”.

Ett ytterligare alternativ är att avgränsa lagen till förberedelse eller stämpling till brott av viss allvarlighetsgrad, t.ex. genom att ange att lagen gäller ”allvarligt brott", eller genom att ange en viss straffskala. Uttrycket allvarligt brott förekommer i ett antal författningar och innebörden varierar beroende på den kontext där uttrycket förekommer. Ett exempel där uttrycket allvarligt brott förekommer är i lagen (2017:496) om internationellt polisiärt samarbete som gäller operativt samarbete enligt avtalet med Finland (4 b kap. 1 §). Enligt propositionen kan en utgångspunkt för bedömningen av om det är fråga om ett allvarligt brott vara att det rör sig om ett konkret brott med ett straffvärde motsvarande minst

fängelse i sex månader (prop. 2024/25:12 s. 24). I brottsbalken är allvarlig brottslighet och liknande uttryck vanligt förekommande som en omständighet som kan göra att ett brott ska rubriceras som grovt. Även där har uttrycket olika betydelse beroende på i vilket straffstadgande det förekommer. När det gäller sådant våld eller hot av allvarligare slag som kan innebära att ett olaga tvång eller våld eller hot mot tjänsteman ska rubriceras som grovt anges t.ex. i förarbetena ett straffvärde om sex månaders fängelse som utgångspunkt. I bestämmelsen om utpressning är motsvarande utgångspunkt sådant våld som avses i 3 kap. 6 § om grov misshandel, men också våld av något mindre allvarligt slag omfattas (se prop. 2015/16:113 s. 82 f., 87 och 92). I 29 kap. 1 § brottsbalken anges vissa allmänna grunder för straffmätning. Där föreskrivs bl.a. att det vid bedömningen av ett brotts straffvärde särskilt ska beaktas om gärningen inneburit ett allvarligt angrepp på någons liv eller hälsa eller trygghet till person. I förarbetena anges att med allvarligt angrepp avses sådana gärningar vars straffvärde motsvarar åtminstone sex månaders fängelse (prop. 2009/10:147 s. 14 f. och 41 f.). Som exempel på brottstyper som omfattas av uttrycket anges bl.a. grov misshandel och annan misshandel av allvarligare slag, människorov, olaga frihetsberövande, grov kvinnofridskränkning, grov fridskränkning, rån, grovt rån samt grövre fall av olaga tvång, olaga hot, utpressning, våld eller hot mot tjänsteman och övergrepp i rättssak.

När det gäller att bedöma frågan om visst rekryteringsinnehåll bör avlägsnas är det fråga om att ingripa i ett tidigt skede. Att då föreskriva att bedömningen ska göras med utgångspunkt i brottets straffvärde framstår som mindre lämpligt. Det skulle ställa krav på mer ingående bedömningar av den gärning som rekryteringen avser som är svåra att göra i det skedet. Mot den bakgrunden framstår det som ändamålsenligt att bedömningen i stället ska göras utifrån straffskalan för det aktuella brottet. En hänvisning till brottets straffskala är vanligt förekommande när det gäller förutsättningarna för att vidta tvångsmedel. För att lagstiftningen ska omfatta sådana brott som är vanligt förekommande vid onlinerekrytering och samtidigt innebära en rimlig avvägning mot de motstående intressen som behöver värnas bör det krävas att det är fråga om rekrytering till ett brott för vilket det är föreskrivet fängelse i två år eller mer. Det som är avgörande är alltså den straffskala som är föreskriven för det

brott som rekryteringen avser. Därutöver krävs att brottet är straffbart på förberedelse- eller stämplingsstadiet. Som exempel på brott som kommer att omfattas kan nämnas mord, misshandel av allvarligare slag, mordbrand, allmänfarlig ödeläggelse, narkotikabrott, grova vapenbrott och grova brott mot lagen (2010:1011) om brandfarliga och explosiva varor. Med denna utformning kommer det sakna betydelse om brottet har fullbordats eller inte. Även innehåll som i praktiken kan vara att bedöma som anstiftan till brott kommer att omfattas förutsatt att brottet är straffbart på stämplings- eller förberedelsestadiet.

Intresset av att kunna avlägsna innehåll som syftar till att rekrytera personer för att begå brott väger tungt. Med den utformning som föreslås bedöms regelverket vara proportionerligt i förhållande till den begränsning av yttrande- och informationsfriheten som det innebär.

Regleringen bör även träffa innehåll som utgör ett led i involverande av en underårig i brottslig verksamhet

Att involvera barn och unga i brottslig verksamhet har av lagstiftaren ansetts så allvarligt att ett eget brott infördes i juli 2023 (16 kap. 5 a § brottsbalken). Straffbestämmelsen innebär att den som för brott eller brottslig verksamhet anlitar, betalar, instruerar eller överlämnar egendom till någon som inte har fyllt arton år och därigenom, eller på annat liknande sätt, involverar honom eller henne i brottet eller den brottsliga verksamheten, döms för involverande av en underårig i brottslighet. Bestämmelsen är tillämplig även om den som begår en sådan gärning inte haft uppsåt till men varit oaktsam beträffande omständigheten att den andra personen inte fyllt arton år. Om involverandet med hänsyn till den ringa skillnaden i ålder eller utveckling mellan gärningspersonen och den andra personen, eller annars är uppenbart mindre allvarligt ska inte dömas till ansvar.

Den straffbara gärningen kan bestå i att den unge används, beordras eller hörsammar en uppmaning om att utföra en handling som har betydelse vid utförandet av ett brott, som t.ex. att genomföra eller hålla vakt vid ett rån. Det kan också handla om att den unge betalas, med t.ex. pengar eller föremål, för att utföra en tjänst som är brottslig, som att sälja eller transportera narkotika.

Även den som t.ex. lämnar instruktioner för brott eller brottslig verksamhet eller erbjuder betalning eller annan förmån för en tjänst som är brottslig omfattas av straffansvar, liksom den som uppmuntrar den unge att agera på ett sätt som har betydelse vid utförandet av ett brott.

Avsikten med straffbestämmelsen är att de som på olika sätt bidrar till att unga dras in i kriminalitet ska kunna lagföras. Det krävs inte att gärningen innefattat tvång, vilseledande, övertalning eller liknande. Att den unge av fri vilja och kanske till och med på eget initiativ deltar i brott eller brottslig verksamhet utesluter alltså inte ansvar för den som kan sägas ha involverat den unge. För straffansvar krävs inte heller att den unge begått någon straffbelagd handling. Redan den som t.ex. har anlitats eller betalats, eller gått med på ett erbjudande om betalning, kan ha blivit involverad i brottslig verksamhet. Förfarandet att involvera den unge måste dock vara reellt på så vis att denne accepterat att anlitas eller betalats för brottslig verksamhet. Den som t.ex. endast uppmanar någon att delta i brottslig verksamhet har däremot inte involverat den unge innan det står klart att denne har hörsammat uppmaningen.

Straffet för brottet är fängelse i högst fyra år. Att straffskalan sträcker sig till fyra års fängelse medger att straffvärdet i det enskilda fallet kan sättas högre än det som följer av sådan brottslighet som den unge gjort sig skyldig till. Någon korrelation behöver alltså inte råda mellan straffvärdet för att ha involverat en ung person i brottslighet och den aktuella brottslighetens straffvärde.

Straffbestämmelsen är tillämplig när en gärning även är straffbar som anstiftan eller stämpling till brott. I dessa fall ska det i regel dömas i konkurrens, dvs. både för medverkan till det brott som den unge begått och för involverande av en underårig i brottslighet (prop. 2022/23:53 s. 147).

Det är särskilt angeläget att kunna bryta onlinerekryteringen av barn och unga. Det gäller även om det är fråga om rekrytering till mindre allvarlig brottslighet. Ett barn eller en ungdom som har rekryterats för att utföra ett mindre allvarligt brott löper hög risk för att genom påtryckningar eller på annat sätt dras in i mer allvarlig kriminalitet. Innehåll som innefattar involverande av en underårig i brottslighet behöver därför kunna bli föremål för ett föreläggande om avlägsnande. Något krav på att det ska vara fråga om brott av viss allvarlighetsgrad bör alltså inte gälla vid rekrytering av barn och

unga. Det bör inte heller krävas att det uppdrag som annonseras ut är straffbart på förberedelse- eller stämplingsstadiet. Den nya lagstiftningen bör därför utformas på så sätt att den omfattar även innehåll som utgör ett led i ett involverande av en underårig i brottslighet enligt 16 kap. 5 a § brottsbalken.

Vilket beviskrav bör gälla?

För att lagstiftningen ska vara proportionerlig och inte innebära ett för långtgående ingrepp i yttrande- och informationsfriheten ska den som framgår ovan begränsas till att omfatta innehåll som syftar till att rekrytera någon för att begå ett brott för vilket det är föreskrivet fängelse i två år eller mer eller till rekrytering av barn eller unga.

För att den nya lagen ska utgöra ett effektivt verktyg för att motverka onlinerekrytering måste lagen dock kunna tillämpas i ett tidigt skede då det inte finns så mycket information om det brott som rekryteringen avser. Innehåll behöver vidare kunna tas bort även om det i det enskilda fallet kan vara svårt att bedöma avsändarens uppsåt eller om farerekvisitet i 23 kap. 2 § brottsbalken är uppfyllt. De rekryteringsannonser som läggs ut online är ofta allmänt hållna, även om det många gånger i vart fall indirekt framgår vilken typ av brottslighet det är fråga om och vilken ersättning som erbjuds. Ett exempel på innehåll som Polismyndigheten menar är vanligt förekommande är s.k. dödslistor. På ett konto på sociala medier kan det exempelvis läggas ut en rad inlägg i följd med bilder på olika personer och vid respektive person anges en summa åtföljt av en pistol-emoji och därefter, i ytterligare inlägg, anges att den som vill ha uppdraget ska höra av sig. Dödslistorna får ofta spridning genom att andra konton länkar till kontot som publicerat listan och uppmanar andra att följa det.

Med hänsyn till hur rekryteringsannonserna vanligtvis är utformade är det viktigt att kraven i bevishänseende inte sätts för högt, eftersom det annars inte kommer vara möjligt att avlägsna innehållet. Ett för högt ställt beviskrav skulle också kunna leda till att de kriminella enkelt kan anpassa utformningen av annonserna för att komma runt lagstiftningen.

Ett alternativ är att ställa upp motsvarande beviskrav som gäller för att inleda förundersökning, d.v.s. ”anledning att anta” (23 kap. 1 § rättegångsbalken). Detta beviskrav motsvarar vad som gäller för vissa tvångsmedel som biometrisk autentisering, husrannsakan och genomsökning på distans (27 kap. 17 f §, 28 kap. 1 § och 10 b § rättegångsbalken). Att innehåll som kan leda till att en förundersökning inleds också kan tas bort från internet framstår i och för sig som rimligt. Samtidigt innebär en sådan åtgärd ett ingrepp i yttrande- och informationsfriheten. Tröskeln för när innehåll kan bli föremål för ett avlägsnande bör därför inte sättas för lågt. Det lämpligaste alternativet för att åstadkomma en rimlig avvägning i detta avseende är att använda beviskravet ”skäligen kan antas”, vilket motsvarar det beviskrav som gäller för att t.ex. ta ett föremål i beslag (27 kap. 1 § rättegångsbalken). Det innebär att det i det enskilda fallet ska finnas någon konkret omständighet som med viss styrka tyder på att syftet med innehållet är att rekrytera någon för att utföra ett brott och att det är fråga om ett sådant brott som omfattas av lagstiftningen.

När det gäller involverande av en underårig i brottslighet innebär kravet att det inte behöver slås fast att syftet med innehållet varit att rekrytera en person under 18 år och att en underårig person åtagit sig att utföra gärningen. Det är tillräckligt att det framgår av sammanhanget att innehållet riktat sig till eller varit tillgängligt för personer under 18 år och att det finns någon konkret omständighet som med viss styrka tyder på att någon har åtagit sig att utföra gärningen eller på annat sätt hörsammat uppmaningen och att denne är under 18 år.

Om beviskravet är uppfyllt i det enskilda fallet får bedömas utifrån en helhetsbedömning med beaktande av innehållet i sig, dess kontext, var innehållet publicerats, vem som är avsändare, mottagarkretsen etc. Vid denna bedömning kan flera inlägg som publicerats i en följd eller på annat sätt i ett sammanhang behöva bedömas gemensamt.

4.3 Lagen ska endast gälla rekryteringsinnehåll som har anknytning till Sverige

Förslag

Lagen ska endast gälla rekryteringsinnehåll som riktar sig till personer i Sverige eller avser brott som ska begås här eller mot en svensk medborgare eller någon som har hemvist i Sverige

Skälen för förslaget

Enligt förordningen om digitala tjänster kan förelägganden att agera mot olagligt innehåll riktas även till leverantörer av förmedlingstjänster som är etablerade i en annan medlemsstat. Samtidigt ska det territoriella tillämpningsområdet för sådana förelägganden fastställas tydligt på grundval av tillämplig unionsrätt eller nationell rätt som möjliggör utfärdandet av föreläggandet och bör inte gå utöver vad som är strikt nödvändigt för att uppnå dess mål (artikel 9).

Det bör mot denna bakgrund krävas att innehållet som sådant har anknytning till svenska intressen för att ett föreläggande om avlägsnande ska kunna beslutas av en svensk myndighet. Detta bör framgå av lagstiftningen. Mot vem ett föreläggande om avlägsnande av rekryteringsinnehåll ska riktas behandlas i avsnitt 5.1.

För att förelägganden om att avlägsna rekryteringsinnehåll ska vara ett effektivt verktyg för att motverka onlinerekryteringen bör det vara möjligt att besluta ett sådant föreläggande beträffande både innehåll som tar sikte på rekrytering av svenskar till brott och innehåll som avser rekrytering till brott som planeras att utföras i Sverige eller mot en svensk person. När det gäller att brottsoffret är en svensk person bör detta uttryckas på samma sätt som i 2 kap. 3 § brottsbalken avseende svensk domstols behörighet. Det bör alltså krävas att den person som brottet planeras att riktas mot är svensk medborgare eller någon som har hemvist i Sverige. Lagen ska alltså sammanfattningsvis vara tillämplig såväl på innehåll som riktar sig till personer i Sverige som innehåll som avser brott som ska begås här i landet eller mot en svensk medborgare eller någon annan person med hemvist i Sverige.

Eftersom det är fråga om innehåll som publiceras online kan det vara svårt att avgöra om innehållet är riktat till personer i Sverige. För att bedöma om kravet är uppfyllt kommer det behöva göras en helhetsbedömning utifrån innehållet som sådant och dess kontext, var det publicerats etc. I princip allt innehåll som publiceras online är tillgängligt för personer här i landet. Enbart teknisk åtkomst kan därför inte vara tillräckligt. Kravet bör däremot normalt anses uppfyllt om innehållet publiceras på en plattform eller domän med tydlig anknytning till Sverige. Detsamma får anses gälla för innehåll som publiceras på andra domäner eller plattformar om det framgår av innehållet eller sammanhanget i övrigt att det som publicerats riktar sig till personer i Sverige. Även innehåll som inte riktar sig till personer i Sverige kan omfattas om det t.ex. av innehållet som sådant eller av dess sammanhang framgår att det är fråga om rekrytering till ett brott som planeras att utföras i Sverige eller mot en svensk person.

4.4 Undantag för terrorisminnehåll

Förslag

Lagen ska inte vara tillämplig på innehåll som omfattas av TCO-förordningen.

Skälen för förslaget

För sådant innehåll som utgör terrorisminnehåll enligt TCO-förordningen gäller bestämmelserna i förordningen och TCO-lagen. Material som utgör terrorisminnehåll kan i vissa fall samtidigt vara att betrakta som sådant rekryteringsinnehåll som omfattas av den nya lagen. För att det inte ska råda oklarhet kring vilket regelverk som är tillämpligt, och för att undvika risken att den nya lagen i något avseende står i strid med TCO-förordningen, bör det i den nya lagen föreskrivas att lagen inte gäller för sådant innehåll som omfattas av TCO-förordningen.

5 Förelägganden om avlägsnande

5.1 En möjlighet att besluta förelägganden om avlägsnande införs

Förslag

En behörig myndighet som regeringen bestämmer ska kunna förelägga en värdtjänstleverantör att avlägsna rekryteringsinnehåll.

Skälen för förslaget

Förelägganden ska beslutas av en behörig myndighet som bestäms av regeringen

Som framgår av föregående avsnitt bör lagstiftningen utformas med TCO-förordningen som förebild. Det innebär att den nya lagen om avlägsnande av rekryteringsinnehåll behöver ge rättsligt stöd för att besluta förelägganden om att sådant innehåll ska tas bort eller göras oåtkomligt. En nationell lagstiftning om avlägsnande av rekryteringsinnehåll online behöver utformas med beaktande av förordningen om digitala tjänster. I artikel 9 i förordningen finns bestämmelser om förelägganden att agera mot olagligt innehåll. Ett sådant föreläggande kan enligt förordningen beslutas av berörda nationella rättsliga eller administrativa myndigheter. Uppgiften att besluta om förelägganden om avlägsnande av rekryteringsinnehåll enligt den nya lagen bör ges till en utpekad behörig myndighet.

Regeringen har utsett Polismyndigheten till svensk behörig myndighet enligt TCO-förordningen. Det framstår som lämpligt att

samma myndighet även utses till behörig myndighet när det gäller att besluta föreläggande om avlägsnande enligt den nya lagen. Polismyndighetens uppdrag när det gäller TCO-förordningen är inte reglerat i lag utan i myndighetens instruktion. Även när det gäller den nya lagen bör den behöriga myndigheten pekas ut i förordning. Det ska därför anges i den nya lagen att ett föreläggande om avlägsnande får beslutas av den myndighet som regeringen bestämmer.

Ett föreläggande om avlägsnande ska riktas till en värdtjänstleverantör

När det gäller frågan till vem ett föreläggande om att avlägsna rekryteringsinnehåll ska riktas finns det anledning att titta på hur både förordningen om digitala tjänster och TCO-förordningen är utformade.

Förordningen om digitala tjänster är tillämplig på leverantörer av s.k. förmedlingstjänster. En förmedlingstjänst är en typ av informationssamhällestjänst. I artikel 3 definieras informationssamhällestjänst genom en hänvisning till definitionen i artikel 1.1 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. Informationssamhällets tjänster omfattar enligt direktivet alla tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I bestämmelsen finns vidare följande definitioner:

i) på distans: tjänster som tillhandahålls utan att parterna är närvarande samtidigt,

ii) på elektronisk väg: en tjänst som sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling och lagring av uppgifter, och som i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel,

iii) på individuell begäran av en tjänstemottagare: en tjänst som tillhandahålls genom överföring av uppgifter på individuell begäran.

De förmedlingstjänster som omfattas av förordningen om digitala tjänster definieras i artikel 3. De är uppdelade i kategorierna enbart vidarefordran, cachning, värdtjänster (varav vissa är online-

plattformar av olika storlek) samt mycket stora onlinesökmotorer. Förmedlingstjänster kan exempelvis utgöra en infrastruktur för tredje parts innehåll, vara eller tjänst, t.ex. ett meddelande, en uppladdad video, ett blogginlägg eller en vara som bjuds ut till försäljning (prop. 2023/24:160 s. 19).

Förordningen är tillämplig på förmedlingstjänster som erbjuds till tjänstemottagare som har sitt etableringsställe eller befinner sig i unionen, oavsett var de leverantörer som tillhandahåller dessa förmedlingstjänster har sitt etableringsställe (artikel 2.1). Med att erbjuda tjänster i unionen avses att göra det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda de tjänster som tillhandahålls av en leverantör av förmedlingstjänster som har en väsentlig anknytning till unionen. Väsentlig anknytning till unionen följer antingen av att leverantören är etablerad i unionen eller av särskilda faktiska kriterier, såsom ett betydande antal tjänstemottagare i en eller flera medlemsstater i förhållande till dess eller deras befolkning, eller verksamhet som riktas till en eller flera medlemsstater. Tjänstemottagare definieras som en fysisk eller juridisk person som använder en förmedlingstjänst, i synnerhet för att söka information eller göra den tillgänglig (artikel 3).

TCO-förordningen är tillämplig på s.k. värdtjänstleverantörer. Begreppet värdtjänstleverantör definieras, delvis genom en hänvisning till ovan nämnda direktiv 2015/1535, som en leverantör av någon av alla informationssamhällets tjänster som består i att information som tillhandahållits av en innehållsleverantör lagras på dennes begäran (artikel 2.1). Med informationssamhällets tjänster avses tjänster som vanligtvis utförs mot ersättning (dvs. kommersiella tjänster) på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I skälen till förordningen utvecklas begreppet något: Förordningen bör tillämpas på sådana leverantörer av 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 är av rent teknisk, automatisk och passiv karaktär. Begreppet lagring bör förstås som förvaring av data i minnet hos en fysisk eller virtuell server (skäl 13). Det innebär att förordningen exempelvis bör omfatta leverantörer av sociala medietjänster, video, bild- och 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 14).

TCO-förordningen är tillämplig på värdtjänstleverantörer som erbjuder tjänster i EU, oberoende av deras huvudsakliga verksamhetsställe, i den mån de sprider information till allmänheten (artikel 1.2). Med detta avses att göra det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda de tjänster som erbjuds av en värdtjänstleverantör som har en betydande anknytning till den eller de medlemsstaterna (artikel 2.4). Betydande anknytning innebär i sin tur att en värdtjänstleverantör har en anknytning till en eller flera medlemsstater som följer antingen av dennes verksamhetsställe i unionen eller av särskilda faktiska kriterier. Dessa kriterier kan vara att värdtjänstleverantören har ett betydande antal användare av dess tjänster i en eller flera medlemsstater eller att verksamheten är riktad mot en eller flera medlemsstater (artikel 2.5).

Förordningen om digitala tjänster har alltså ett vidare tillämpningsområde än TCO-förordningen när det gäller vilka aktörer som kan bli föremål för ett föreläggande om att ta bort olagligt innehåll. Ett föreläggande om att avlägsna rekryteringsinnehåll som riktas mot en sådan aktör som omfattas av förordningen om digitala tjänster kommer att träffas av artikel 9 i förordningen. Detta kan anses tala för att ett föreläggande om att ta bort rekryteringsinnehåll bör kunna skickas till samtliga aktörer som omfattas av förordningen om digitala tjänster. Det är dock inte givet att alla aktörer som omfattas av förordningen verkligen har möjlighet att avlägsna visst innehåll. Det skulle också underlätta tillämpningen om regleringen är avgränsad på motsvarande sätt som TCO-förordningen, dvs. på så sätt att endast leverantörer av sådana förmedlingstjänster som utgör värdtjänster kan bli föremål för ett föreläggande. Ett avgränsande till värdtjänstleverantörer innebär att föreläggandet ska riktas till den som tillhandahåller den tjänst där informationen finns och inte till den som skapat innehållet eller lagt ut det på internet. En sådan avgränsning träffar alltså den krets av aktörer, tex. plattformar för social media eller för delning av innehåll, som normalt bör ha möjlighet att ta bort innehållet (jfr skäl 27 i förordningen om digitala tjänster). Sammantaget bör förelägganden enligt den nya lagen riktas mot värdtjänstleverantörer. Avgränsningen bör göras på så sätt att det i lagen anges att med värdtjänst-

leverantör avses en sådan leverantör av värdtjänster som omfattas av förordningen om digitala tjänster. För att omfattas av den nya lagen krävs alltså bl.a. att värdtjänstleverantören erbjuder tjänster till tjänstemottagare i unionen och att värdtjänsten har väsentlig anknytning till unionen. Att en webbplats är tekniskt åtkomlig i unionen är inte tillräckligt. Som framgår av avsnitt 4.2 och 4.3 krävs vidare att rekryteringsinnehållet sprids till allmänheten och att det har anknytning till Sverige för att ett föreläggande ska kunna beslutas. Ett föreläggande om avlägsnande kan riktas även till en värdtjänstleverantör som är etablerad i en annan medlemsstat.

Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En följd av denna hänvisningsteknik är att den nationella författningen normalt behöver ändras varje gång EU-bestämmelsen ändras. En dynamisk hänvisning innebär i stället att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. När det gäller hänvisningen till begreppet värdtjänst bör eventuella ändringar i förordningen få omedelbart genomslag i regleringen. Hänvisningen till förordningen om digitala tjänster ska därför vara dynamisk.

5.2 Förelägganden ska utformas i enlighet med förordningen om digitala tjänster

Förslag

Ett föreläggande om avlägsnande av rekryteringsinnehåll ska uppfylla de krav som följer av artikel 9.2 i förordningen om digitala tjänster. Det ska i den nya lagen upplysas om att artikel 9 i förordningen innehåller bestämmelser om förfarandet efter beslut om ett föreläggande.

Skälen för förslaget

Ett föreläggande om att ta bort rekryteringsinnehåll enligt den nya lagen kommer att utgöra ett sådant föreläggande som avses i

artikel 9.1 i förordningen om digitala tjänster. Enligt artikel 9.2 ska medlemsstaterna säkerställa att ett föreläggande att agera mot olagligt innehåll uppfyller vissa villkor när det översänds till leverantören. Föreläggandet ska bl.a. innehålla

1. en hänvisning till den rättsliga grunden för föreläggandet, i unionsrätt eller nationell rätt,
2. en motivering som förklarar varför informationen utgör olagligt innehåll, med hänvisning till en eller flera specifika bestämmelser i unionsrätt eller nationell rätt i överensstämmelse med unionsrätten,
3. information som identifierar den utfärdande myndigheten,
4. tydlig information som gör det möjligt för leverantören av förmedlingstjänster att identifiera och lokalisera det berörda olagliga innehållet, såsom en eller flera URL och, när så är nödvändigt, ytterligare information,
5. information om de prövningsmekanismer som finns tillgängliga för leverantören av förmedlingstjänster och för den tjänstemottagare som tillhandahållit innehållet, och
6. i tillämpliga fall, upplysningar om vilken myndighet som ska få informationen om den verkan som ges åt föreläggandena.

Artikel 9.2 i förordningen om digitala tjänster förutsätter kompletterande bestämmelser i nationell rätt. Det ska därför i den nya lagen införas en bestämmelse som reglerar kraven som ett sådant föreläggande ska uppfylla. Det kan göras genom en hänvisning till kraven i artikel 9.2 i förordningen. Hänvisningen till förordningen bör vara dynamisk. Det innebär att den avser förordningen i den vid varje tidpunkt gällande lydelsen.

Enligt artikel 9.1 i förordningen om digitala tjänster ska leverantörer av förmedlingstjänster vid mottagandet av ett föreläggande vilket utfärdats av de berörda nationella rättsliga eller administrativa myndigheterna, utan onödigt dröjsmål informera den myndighet som utfärdade föreläggandet eller annan eventuell myndighet som anges i föreläggandet om varje eventuell verkan det givits, med angivande av om och när föreläggandet getts verkan. Enligt artikel 9.3 ska den utfärdande myndigheten eller den myndighet som anges i föreläggandet översända föreläggandet och informationen som myndigheten mottagit till samordnaren för digitala tjänster i den utfärdande myndighetens medlemsstat. I enlighet med artikel 9.4 ska sedan samordnaren för digitala tjänster

översända en kopia av föreläggandet till alla andra samordnare för digitala tjänster. Slutligen ska leverantörer av förmedlingstjänster enligt artikel 9.5 vid en viss tidpunkt informera den berörda tjänstemottagaren om det mottagna föreläggandet och den verkan det givits, samt viss annan information.

Bestämmelserna i artiklarna 9.1, 9.3, 9.4 och 9.5 i förordningen om hur förelägganden ska hanteras och följas upp är direkt tillämpliga. För att underlätta för myndigheter och domstolar som ska utfärda förelägganden och ta emot information om uppföljning har en upplysningsbestämmelse om dessa regler införts i lagen (2024:954) med kompletterande bestämmelser till EU:s förordning om digitala tjänster. En motsvarande upplysningsbestämmelse bör tas in i den nya lagen om avlägsnande av rekryteringsinnehåll online.

Den värdtjänstleverantör som mottagit ett föreläggande om att avlägsna visst innehåll ska senast vid den tidpunkt då föreläggandet ges verkan eller, i förekommande fall, vid den tidpunkt som den utfärdande myndigheten anger i sitt föreläggande, informera den berörda tjänstemottagaren om det mottagna föreläggandet och den verkan det givits. Sådan information som tillhandahålls tjänstemottagaren ska innehålla en motivering, ange de möjligheter till prövning som finns och en beskrivning av det territoriella tillämpningsområdet för föreläggandet (artikel 9.5). Enligt skälen till förordningen kan skyldigheten för leverantörer av förmedlingstjänster att informera tjänstemottagaren senareläggas i enlighet med tillämplig unionsrätt eller nationell rätt, särskilt i samband med straffrättsliga, civilrättsliga eller administrativa förfaranden (skäl 34).

Det kan med hänsyn till exempelvis en pågående förundersökning vara nödvändigt att kunna skjuta upp tidpunkten för när information ska lämnas till tjänstemottagaren. Bestämmelser som möjliggör detta behöver därför kunna införas (jfr artikel 11 TCO-förordningen). Detta kan regleras på lägre författningsnivå än lag.

5.3 Avlägsnande av rekryteringsinnehåll

Förslag

En värdtjänstleverantör som mottar ett föreläggande om avlägsnande ska avlägsna rekryteringsinnehållet eller göra det oåtkomligt så snart som möjligt och senast inom en timme från mottagandet av föreläggandet.

Om det är tillräckligt att innehållet görs oåtkomligt i en eller flera stater ska den behöriga myndigheten ange det i föreläggandet.

Skälen för förslaget

Mottagaren av en avlägsnandeorder är enligt TCO-förordningen skyldig att avlägsna terrorisminnehållet eller göra innehållet oåtkomligt så snart som möjligt och i alla händelser inom en timme från mottagandet av ordern. Ett syfte med den nya lagen är att bryta de kriminella gängens rekrytering, inte minst av barn och unga. För att lagen ska få effekt krävs att rekryteringsinnehållet tas bort så snart som möjligt. Tidsfristen för att avlägsna innehållet eller göra det oåtkomligt bör därför motsvara vad som gäller enligt TCO-förordningen. Innehållet ska alltså tas bort så snart som möjligt och senast inom en timme från mottagandet av ett föreläggande.

Enligt TCO-förordningen ska materialet göras oåtkomligt i alla medlemsstater. I direktivet om bekämpning av våld mot kvinnor och våld i nära relationer har en annan lösning valts. I direktivet anges att materialet ska göras oåtkomligt utan angivande av territoriellt område.

Enligt förordningen om digitala tjänster bör föreläggandets verkan, i synnerhet i ett gränsöverskridande sammanhang, i princip begränsas till den utfärdande medlemsstatens territorium, såvida inte innehållets olaglighet härrör direkt från unionsrätten eller den utfärdande myndigheten anser att de rättigheter som står på spel kräver ett bredare territoriellt tillämpningsområde, i enlighet med unionsrätten och internationell rätt, samtidigt som principen om internationell hövlighet beaktas (artikel 9 och skäl 36).

Det kan antas att de föreläggande om att ta bort rekryteringsinnehåll som kommer att beslutas med stöd av den nya lagen i många fall kommer att avse innehåll som är riktat till personer i Sverige. Det kan då vara tillräckligt att innehållet görs oåtkomligt i Sverige för att föreläggandet ska få avsedd effekt. Samtidigt ska ett föreläggande också kunna beslutas beträffande innehåll som inte är riktat mot personer i Sverige, om det avser brott som planeras att utföras i Sverige eller mot en svensk person. Som exempel kan nämnas innehåll där avsikten är att rekrytera personer i Danmark för att begå brott i Sverige eller mot en svensk person. I dessa fall kommer det inte vara tillräckligt att innehållet görs oåtkomligt i Sverige. Utgångspunkten i lagen bör därför vara att rekryteringsinnehåll ska avlägsnas eller göras oåtkomligt utan begränsning till visst territoriellt område. Om den behöriga myndigheten gör bedömningen i det enskilda fallet att det är tillräckligt att innehållet görs oåtkomligt i en eller flera stater, t.ex. Sverige och Danmark, ska myndigheten ange det i föreläggandet. Eftersom lagen avgränsas till leverantörer av värdtjänster som omfattas av förordningen om digitala tjänster kommer det endast att bli fråga om att göra material oåtkomligt inom en eller flera av EU:s medlemsstater.

5.4 Bevarande av rekryteringsinnehåll

Förslag

En värdtjänstleverantör ska bevara det rekryteringsinnehåll, samt tillhörande data, som har avlägsnats eller gjorts oåtkomligt till följd av ett föreläggande om avlägsnande.

Rekryteringsinnehållet och tillhörande data ska bevaras i sex månader från det att innehållet avlägsnats eller gjorts oåtkomligt.

Skälen för förslaget

Enligt TCO-förordningen ska värdtjänstleverantörer i sex månader bevara sådant terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder. Även tillhörande data

som är nödvändiga för administrativa eller rättsliga prövningsförfaranden, hantering av klagomål eller för förebyggande, förhindrande, upptäckt, utredning och lagföring av terroristbrott ska bevaras under samma tid (artikel 6). Skyldigheten att bevara materialet för utrednings- eller lagföringsändamål motiveras av att bevarandet är nödvändigt med tanke på det värde som materialet kan tillföra för att störa eller förhindra terroristverksamhet (skäl 27).

Motsvarande bör gälla för rekryteringsinnehåll enligt den nya lagen. En skyldighet att bevara rekryteringsinnehåll som har avlägsnats eller gjorts oåtkomligt bör alltså införas. På samma sätt som enligt TCO-förordningen bör skyldigheten att bevara uppgifter även omfatta tillhörande data. Det innebär att exempelvis uppgifter om identitet och IP-adress för den som publicerat innehållet samt datum och tidpunkt för publiceringen ska bevaras (jfr skäl 26 till TCO-förordningen). Skyldigheten att bevara rekryteringsinnehållet och tillhörande data motiveras av att materialet kan behövas för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Vidare föreslås i kommande avsnitt dels att en värdtjänstleverantör som åsidosätter sina skyldigheter enligt den nya lagen ska kunna åläggas sanktionsavgift (avsnitt 7), dels att ett beslut om föreläggande ska kunna överklagas (avsnitt 9). Rekryteringsinnehållet och tillhörande data kan behövas även för prövningen av sådana förfaranden.

6 Förhållandet till yttrande- och informationsfrihet

6.1 Den nya lagens förhållande till tryckfrihetsförordningen och yttrandefrihetsgrundlagen

Bedömning

Den nya lagen ska inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Det behöver inte införas en uttrycklig upplysning om detta.

Bestämmelserna i den nya lagen är förenliga med regeringsformens bestämmelser om yttrande- och informationsfrihet.

Skälen för bedömningen

Innehåll som faller under mediegrundlagarna omfattas inte

Den nya lagen ska gälla rekryteringsinnehåll som sprids till allmänheten genom att publiceras på internet. Som redogörs för i avsnitt 3.1 kan samtidigt innehåll som publiceras på internet i vissa fall omfattas av tryckfrihetsförordningen eller, framför allt, yttrandefrihetsgrundlagen (nedan benämnda mediegrundlagarna). Sådant rekryteringsinnehåll som kommer att omfattas av den nya lagen kan därför i vissa fall vara tillhandahållet på medier som omfattas av mediegrundlagarna. I sådana fall följer redan av mediegrundlagarna att innehåll som skyddas av dessa inte kan bli föremål för någon åtgärd med stöd av den nya lagen – ett

föreläggande om avlägsnande kan alltså inte beslutas avseende sådant innehåll. Detta är en konsekvens av principen om normhierarki, dvs. att grundlagarna har företräde framför vanlig lag. Det finns normalt sett inte något behov av att i vanlig lag ta in en upplysning om grundlagarnas företräde. Undantagsvis kan en sådan upplysningsbestämmelse vara betydelsefull när det finns ett särskilt behov av att tydligt markera en begränsning i fråga om tillämpningsområdet för en viss lag. Det får dock som utgångspunkt anses mindre lämpligt att ta in sådana bestämmelser i en lag när de inte har någon egentlig materiell funktion. I tidigare lagstiftningssammanhang har det diskuterats om det, för att uppmärksamma tillämparen på grundlagarna, bör göras en uttrycklig hänvisning till att dessa gäller. Det har emellertid ansetts att det i regel inte är lämpligt att tynga lagstiftningen med en upplysning om vad som gäller enligt grundlagarna (se t.ex. prop. 2010/11:158 s. 65, prop. 2022/23:42 s. 38–39 och prop. 2025/26:4 s. 30–31). I detta fall talar övervägande skäl emot att i den nya lagen ta in en upplysningsbestämmelse som hänvisar till mediegrundlagarna. För berörda aktörer får det antas stå klart att den nya lagen inte kan tillämpas på innehåll som omfattas av mediegrundlagarna.

Förslagen är förenliga med bestämmelserna om yttrande- och informationsfriheten

Innehåll som kommer att omfattas av den nya lagen och som inte omfattas av skyddet i någon av mediegrundlagarna, omfattas i stället av det allmänna skyddet för yttrande- och informationsfrihet i regeringsformen. De åtgärder som ska kunna vidtas med stöd av den nya lagen innebär inskränkningar i yttrandefriheten för den som publicerar innehållet och i informationsfriheten för mottagarna. Yttrande- och informationsfriheten enligt regeringsformen är emellertid inte absolut utan kan begränsas genom lag, under förutsättning att det rör sig om en proportionerlig inskränkning som sker i ett godtagbart syfte.

Den begränsning av yttrande- och informationsfriheten som den nya lagen innebär motiveras av mycket angelägna syften, nämligen att hindra att framför allt barn och unga hänsynslöst rekryteras till kriminalitet samt att förhindra allvarliga brott. Samtidigt måste det säkerställas att förslagen inte går för långt i förhållande till andra

viktiga intressen som kan påverkas negativt av förslagen. En intresseavvägning måste alltså göras. Det kan då först konstateras att den utbredda rekryteringen till kriminalitet online och fenomenet crime as a service är en synnerligen allvarlig utveckling. Allt fler och yngre barn rekryteras till att begå brott för de kriminella nätverkens räkning. Våldet har tagit sig allt grövre former och drabbar allt fler utanför de kriminella gängen. Det är helt nödvändigt med kraftfulla insatser för att vända utvecklingen.

För att förslagen inte ska gå för långt och utgöra ett oproportionerligt ingrepp i yttrande- och informationsfriheten har tillämpningsområdet för den nya lagen begränsats på så sätt att den endast ska omfatta innehåll som i sig kan vara brottsligt. Lagen ska vidare endast gälla innehåll som syftar till att rekrytera någon för att begå ett brott för vilket det är föreskrivet fängelse i två år eller mer eller som avser rekrytering av barn eller unga till kriminalitet (se avsnitt 4.2). Genom att lagen avgränsas till innehåll som syftar till att rekrytera personer för att begå brott träffar den inte innehåll som sprids till allmänheten i andra syften, som t.ex. utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte. Detta gäller oberoende av om innehållet omfattas av mediegrundlagarna eller inte. Ett föreläggande om att visst innehåll ska avlägsnas ska vidare kunna överklagas (se avsnitt 9) och det ska införas ett krav på att det rekryteringsinnehåll som avlägsnats ska bevaras, bl.a. för att ett överklagande ska kunna prövas. Sammantaget innebär detta att bestämmelserna i den nya lagen är proportionerliga och utgör en godtagbar begränsning av yttrande- och informationsfriheten enligt regeringsformen. Detsamma gäller motsvarande skydd enligt Europakonventionen och EU:s rättighetsstadga.

7 Sanktionsavgifter

7.1 Den behöriga myndigheten ska kunna besluta om sanktionsavgift

Förslag

Den behöriga myndigheten ska få besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som överträder sina skyldigheter enligt lagen.

Skälen för förslaget

Den nya lagen ger den behöriga myndigheten möjlighet att besluta föreläggande om avlägsnande av rekryteringsinnehåll. En värdtjänstleverantör som mottar ett sådant föreläggande är skyldig att så snart som möjligt, och senast inom en timme från mottagandet, avlägsna rekryteringsinnehållet eller göra det oåtkomligt. Leverantören är dessutom skyldig att bevara det innehåll som avlägsnats, samt tillhörande data (se avsnitt 5.3 och 5.4).

För att säkerställa att den föreslagna regleringen får genomslag behöver det införas någon form av sanktioner vid överträdelser. Sanktionerna behöver vara effektiva och avskräckande. Det är dock inte lämpligt att kriminalisera överträdelser av den nya lagen, eftersom kriminalisering endast bör ske om andra medel är otillräckliga. Den lämpligaste typen av sanktion när det gäller överträdelser av skyldigheterna enligt den nya lagen är i stället sanktionsavgifter. Det motsvarar vad som gäller för motsvarande överträdelser enligt TCO-lagen. Huvudregeln är att sanktionsavgiftssystem bygger på strikt ansvar (prop. 2017/18:232 s. 324),

dvs. att det inte krävs att överträdelser skett uppsåtligen eller av oaktsamhet. En sådan ordning, som alltså innebär att det inte krävs någon prövning av subjektiva rekvisit, skulle bidra till ett effektivt sanktionssystem vid överträdelser av den nya lagen. Sanktionsavgifterna bör därför bygga på ett strikt ansvar – något som inte behöver anges särskilt i lagen.

Frågan är då vem som ska ges befogenhet att besluta om sanktionsavgift. Det finns i praktiken två alternativ: Antingen den behöriga myndigheten eller en domstol, efter ansökan av den behöriga myndigheten. Båda alternativen är vanligt förekommande i liknande regelverk. Generellt sett anses en tillsynsmyndighet lämpad att besluta om sanktionsavgift när reglerna är relativt enkla att tillämpa, beslutsfattandet är förhållandevis schabloniserat och sanktionsbestämmelserna bygger på strikt ansvar. En domstol brukar anses mer lämpad att besluta om sanktionsavgift om det är aktuellt att pröva framför allt subjektiva rekvisit eller andra svårbedömda rekvisit (se t.ex. prop. 2017/18:232 s. 332).

I förarbetena till TCO-lagen konstaterades att även om regleringen i TCO-förordningen bitvis är komplicerad, så gäller inte det i någon större utsträckning tillämpningen av de bestämmelser som ska förenas med sanktionsavgift (prop. 2022/23:71 s. 30). Detsamma gäller för aktuella bestämmelser i den nu föreslagna lagen. I dessa fall är det främst fråga om huruvida ett föreläggande om att avlägsna rekryteringsinnehåll eller en skyldighet att bevara sådant innehåll samt tillhörande data har följts. Som anges ovan krävs ingen prövning av subjektiva rekvisit. Sammantaget innebär detta att det bör vara den behöriga myndigheten som beslutar om sanktionsavgift. Beslutet bör få överklagas till allmän förvaltningsdomstol (se avsnitt 9). På så sätt tillgodoses rättssäkerhetsaspekterna för den som åläggs sanktionsavgift och på sikt kommer det att kunna bildas domstolspraxis till vägledning för myndighetens beslut.

Det kan inte uteslutas att en värdtjänstleverantör kan komma att bli föremål för en straffrättslig process med anledning av rekryteringsinnehåll som sprids på tjänsten, vilket kan aktualisera förbudet mot dubbelprövning. Skulle en sådan situation uppkomma framstår det som givet att det straffrättsliga förfarandet bör ges företräde. Den behöriga myndigheten bör i ett sådant fall alltså avstå

från att besluta om sanktionsavgift, vilket är möjligt eftersom det inte är obligatoriskt att påföra sådan avgift.

7.2 Sanktionsavgiftens storlek

Förslag

En sanktionsavgift ska bestämmas till lägst 5 000 kr och högst 5 000 000 kr eller, vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheten att avlägsna rekryteringsinnehåll eller göra det oåtkomligt, upp till ett sådant högre belopp som motsvarar fyra procent av leverantörens globala omsättning närmast föregående räkenskapsår.

Om en överträdelse som kan leda till högre sanktionsavgift än 5 000 000 kr har skett under leverantörens första verksamhetsår eller om uppgifter om omsättningen annars saknas eller är bristfälliga, får omsättningen uppskattas.

Den behöriga myndigheten får sätta ned sanktionsavgiften helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna framstår som oskäligt att ta ut avgiften.

Skälen för förslaget

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

Utgångspunkten för utformningen av regleringen i den nya lagen bör vara att en sanktionsavgift ska kunna vara effektiv, proportionerlig och avskräckande för samtliga värdtjänstleverantörer, dvs. oavsett om det rör sig om fysiska eller juridiska personer och oavsett om de bedriver en mindre verksamhet med begränsade resurser eller en större verksamhet med mycket stora resurser. Det framstår därför som lämpligt att regleringen utformas

på så vis att sanktionsavgiften ska fastställas till ett belopp inom ett bestämt beloppsintervall.

Förutom att värdtjänstleverantörernas ekonomiska förmåga kan skilja sig mycket åt, kan de överträdelser som kan leda till en sanktionsavgift vara olika allvarliga – från att av oaktsamhet inte bevara en mindre del av den data som leverantören är skyldig att bevara till att helt ignorera ett föreläggande om avlägsnande. Beloppsintervallet bör därför vara förhållandevis stort för att ge den behöriga myndigheten utrymme att göra en nyanserad bedömning av avgiftens storlek i det enskilda fallet. Med hänsyn till detta bör en sanktionsavgift bestämmas till lägst 5 000 kr och högst 5 000 000 kr, vilket också motsvarar vad som enligt TCO-lagen gäller vid åsidosättanden av sådana skyldigheter enligt TCO-förordningen som kan leda till sanktionsavgift.

TCO-lagen innehåller även en särskild beräkningsgrund för sanktionsavgiften när det är fråga om en systematisk eller fortgående underlåtenhet av värdtjänstleverantören att fullgöra sin skyldighet att avlägsna terrorisminnehåll eller göra det oåtkomligt. I sådana fall kan sanktionsavgiften bestämmas till ett sådant högre belopp som motsvarar upp till fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret. Bestämmelsen i TCO-lagen har sin grund i att medlemsstaterna enligt TCO-förordningen har en särskild skyldighet att säkerställa att den typen av överträdelser kan bli föremål för en sanktionsavgift som bestäms på det sättet (se prop. 2022/23:71 s. 31–32). Något skäl att se mindre allvarligt på motsvarande överträdelser av den nu föreslagna lagen finns inte. En värdtjänstleverantör som systematiskt eller fortgående underlåter att avlägsna rekryteringsinnehåll eller göra det oåtkomligt, bör kunna åläggas en sanktionsavgift av samma storlek som en värdtjänstleverantör som på samma sätt underlåter att följa en avlägsnandeorder som avser terrorisminnehåll. Vid sådana överträdelser bör sanktionsavgiften därför kunna bestämmas till ett sådant högre belopp som motsvarar upp till fyra procent av leverantörens globala omsättning närmast föregående räkenskapsår. För det fall att överträdelsen inträffar under leverantörens första verksamhetsår eller att uppgifter om omsättningen av andra skäl saknas eller är bristfälliga, bör omsättningen få uppskattas.

När den behöriga myndigheten ska bestämma sanktionsavgiftens storlek måste en helhetsbedömning göras. Vid bedömningen

behöver hänsyn tas till bl.a. hur allvarlig överträdelsen är och leverantörens finansiella ställning.

Även om en överträdelse i och för sig har skett så kan det finnas skäl att avstå från att ta ut en sanktionsavgift. Det kan exempelvis framstå som oskäligt att ta ut en sanktionsavgift när åsidosättandet är mindre allvarligt. Det bör anges uttryckligen i lagen att den behöriga myndigheten helt eller delvis får sätta ned sanktionsavgiften om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna framstår som oskäligt att ta ut avgiften.

7.3 Förfarandet vid beslut om sanktionsavgift

Förslag

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

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

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

Skälen för förslaget

I och med att den behöriga myndigheten ska besluta om sanktionsavgift kommer förvaltningslagen (2017:900) att gälla för förfarandet. Det behövs dock vissa ytterligare förfarandebestämmelser.

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

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

Det bör framgå uttryckligen av den nya lagen att sanktionsavgiften tillfaller staten. Vidare bör det anges att en sanktionsavgift ska betalas till den behöriga myndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om avgiften inte betalas i tid, ska den behöriga myndigheten lämna den obetalda avgiften för indrivning. Det krävs inte någon särskild föreskrift för att beslutet om sanktionsavgift ska få verkställas enligt utsökningsbalken (se 3 kap. 1 § 6 utsökningsbalken och prop. 2021/22:206).

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

8 Sekretess och dataskydd

Den behöriga myndigheten kommer inom ramen för sitt uppdrag att behöva hantera en mängd uppgifter av olika slag, inklusive sådana som kan vara skyddsvärda. Det behöver därför övervägas om nuvarande sekretessregler ger ett tillräckligt skydd för dessa uppgifter eller om det finns behov av någon ny sekretessbestämmelse.

Vid handläggningen av ett ärende enligt den nya lagen kommer den behöriga myndigheten dessutom att behöva behandla personuppgifter. Det är därför nödvändigt att också analysera hur reglerna förhåller sig till dataskyddsregleringen.

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

8.1 Sekretess hos Polismyndigheten

Förslag

Sekretess ska gälla hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärenden enligt den nya lagen, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. För

uppgift i en allmän handling ska sekretessen gälla i högst sjuttio år.

Bedömning

Det behövs inte någon ny sekretessbestämmelse till skydd för Polismyndighetens brottsbekämpande eller brottsförebyggande verksamhet.

Skälen för förslaget och bedömningen

Polismyndigheten hanterar uppgifter som kan behöva skyddas

De uppgifter som Polismyndigheten kommer behöva hantera inom ramen för ett ärende enligt den nya lagen om avlägsnande av rekryteringsinnehåll kan vara av mycket skilda slag. Förutom mer övergripande uppgifter om exempelvis grupperingar, symboler eller uttryck kan ärendena innehålla texter, bilder eller videor som visar allvarlig brottslighet. De kan också innehålla uppgifter om enskildas personliga intressen, t.ex. om fysiska eller juridiska personers kopplingar till kriminella nätverk eller kriminella aktiviteter. Dessutom kan uppgifter om en värdtjänstleverantörs ekonomiska förhållanden behöva behandlas i ärenden som rör sanktionsavgifter.

Uppgifterna kan vidare komma från en rad olika källor. Förutom att Polismyndigheten själv kan upptäcka rekryteringsinnehåll online, så kan ett ärende enligt den nya lagen komma att inledas exempelvis efter att uppgifter inkommit från allmänheten eller från andra myndigheter.

Ärenden enligt den nya lagen kan beröra grundläggande frågor om yttrandefrihet och det finns därför ett starkt intresse av möjligheter till insyn i dessa. Samtidigt är de uppgifter som Polismyndigheten kommer att hantera känsliga både med hänsyn till allmänna och enskilda intressen. Det måste därför finnas utrymme att skydda vissa uppgifter som Polismyndigheten hanterar inom ramen för ett sådant ärende med sekretess.

Behovet av skydd för allmänna intressen är uppfyllt genom befintliga bestämmelser

När Polismyndigheten handlägger ärenden enligt den nya lagen är det fråga om en form av administrativ handläggning, som inte primärt sker för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott (mer om denna bedömning i avsnitt 8.2). Det innebär att de sekretessregler som gäller inom Polismyndighetens brottsförebyggande och brottsbekämpande verksamhet inte blir tillämpliga enbart på den grunden att uppgifter handläggs inom ramen för ett ärende enligt den nya lagen.

Material som hanteras i ett sådant ärende kommer emellertid, med hänsyn till den typ av innehåll som omfattas av den nya lagen, vara sådant att det kan antas att någon typ av brott planeras eller har begåtts. Polismyndigheten kommer i sådana fall i regel även ha anledning att behandla materialet inom ramen för den brottsförebyggande och brottsbekämpande verksamheten. För uppgifter som behandlas inom ramen för brottsbekämpningen gäller bestämmelserna om sekretess i 18 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400), om det kan antas att syftet med beslutade eller förutsedda åtgärder inom den brottsförebyggande eller brottsbekämpande verksamheten motverkas eller den framtida verksamheten skadas om dessa röjs (1 §) eller om det inte står klart att de kan röjas utan sådana följder (2 §).

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

Det behövs en ny sekretessbestämmelse till skydd för vissa enskilda intressen

Vissa uppgifter om enskildas personliga och ekonomiska förhållanden som kommer att behandlas i ärenden enligt den nya lagen är sådana att ett utlämnande kan få negativa konsekvenser för den enskilde. Att Polismyndighetens handläggning av sådana

ärenden inte kommer att ske inom ramen för myndighetens brottsförebyggande och brottsbekämpande verksamhet innebär emellertid bl.a. att bestämmelsen i 35 kap. 1 § offentlighets- och sekretesslagen, om sekretess för uppgift om en enskilds personliga och ekonomiska förhållanden, i regel inte kommer att kunna tillämpas på uppgifter i ett sådant ärende. Den sekretessbestämmelse som återstår är då den generella bestämmelsen om sekretess till skydd för uppgift om enskilds personliga förhållanden i 21 kap. 1 § offentlighets- och sekretesslagen, men denna är begränsad till uppgifter som rör en enskilds hälsa eller sexualliv. Detta skydd är inte tillräckligt. Det behövs därför en sekretessbestämmelse som skyddar uppgifter om enskilds personliga och ekonomiska förhållanden hos Polismyndigheten i ärenden enligt den nya lagen.

Polismyndigheten kan inom ramen för ett ärende enligt den nya lagen, i likhet med vad som gäller för ärenden enligt TCO-förordningen, komma att hantera uppgifter av mycket varierande slag, vilket gör det svårt att på förhand avgränsa sekretessens föremål alltför mycket utan att samtidigt riskera att skyddsvärda uppgifter faller utanför bestämmelsens tillämpningsområde. Bestämmelsen bör därför, på samma sätt som gäller för ärenden enligt TCO-förordningen, innebära att sekretess ska gälla för uppgift om en enskilds personliga och ekonomiska förhållanden (jfr 35 kap. 23 c § offentlighets- och sekretesslagen). Det vanliga är att sekretessbestämmelser till skydd för uppgifter om enskilda i en verksamhet som avser myndighetsutövning utformas med ett s.k. rakt skaderekvisit, dvs. med en presumtion för att uppgifterna är offentliga. Något skäl för mer långtgående sekretess än så för nu aktuella uppgifter finns inte. Detta motsvarar också vad som gäller för sekretess i ärenden enligt TCO-förordningen. Sekretessen bör därför gälla endast om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Även sekretesstiden bör bestämmas på samma sätt som för ärenden enligt TCO-förordningen, dvs. till högst sjuttio år. Det innebär att sekretessen i ärenden enligt den nya lagen till skydd för enskilda fullt ut bör motsvara den som gäller i ärenden enligt TCO-förordningen. Den enklaste lösningen är därför att utvidga den befintliga sekretessbestämmelsen i 35 kap. 23 c § offentlighets- och sekretesslagen till att även omfatta uppgifter i ärenden enligt den nya lagen. Något skäl att begränsa meddelarfriheten med anledning av den föreslagna

sekretessen finns inte. Slutligen kan det noteras att sekretessen, genom bestämmelsen i 43 kap. 1 § offentlighets- och sekretesslagen, kommer att gälla även vid förvaltningsdomstol när beslut i ett ärende enligt den nya lagen överklagas dit.

8.2 Förhållandet till dataskyddsregleringen

Bedömning

Den nya lagen medför inget behov av ändringar i dataskyddsregleringen.

Skälen för bedömningen

Tillämpligt regelverk för Polismyndigheten

När Polismyndigheten i sin roll som behörig myndighet handlägger ärenden enligt den nya lagen behöver den behandla personuppgifter. Dessa kan finnas i det innehåll som är föremål för granskning, men även i exempelvis en anmälan om rekryteringsinnehåll. Myndigheten kan också behöva behandla personuppgifter som inte berör rekryteringsinnehållet i sig utan som avser berörda innehållsleverantörer och värdjänstleverantörer, de senare inte minst i ärenden om sanktionsavgift.

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

Utfärdandet av förelägganden om avlägsnande av rekryteringsinnehåll har förstås ett nära samband med Polismyndighetens brottsförebyggande och brottsbekämpande verksamhet. Även om det innehåll som ett föreläggande avser är olagligt, så handlar det emellertid i dessa delar om en form av administrativt förfarande som inte sträcker sig längre än att säkerställa att det aktuella innehållet avlägsnas eller görs oåtkomligt. Förfarandet riktar sig dessutom mot värdtjänstleverantörer, dvs. aktörer som i regel inte ansvarar straffrättsligt för det innehåll som sprids på tjänsten. Polismyndighetens personuppgiftsbehandling kan därför inte i dessa delar anses ske primärt i brottsförebyggande eller brottsbekämpande syfte, även om effekterna i förlängningen kan bli positiva för det brottsförebyggande och brottsbekämpande arbetet.

Möjligheterna att besluta om sanktionsavgift vid överträdelser av den nya lagen syftar till att uppnå efterlevnad av lagen, inte till att bestraffa begångna brott. En sanktionsavgift utgör inte en straffrättslig påföljd. Inte heller den personuppgiftsbehandling som Polismyndigheten vidtar i sådana ärenden görs därför i syfte att förebygga eller bekämpa brott i brottsdatalagens mening.

Detta innebär sammantaget att dataskyddsförordningen och dataskyddslagen blir tillämpliga på all behandling av personuppgifter som Polismyndigheten vidtar inom ramen för ett ärende enligt den nya lagen (jfr regeringens bedömning i prop. 2022/23:71, avsnitt 8.4, gällande TCO-ärenden). En annan sak är att vissa personuppgifter i ärenden enligt den nya lagen kan härröra från verksamhet vid Polismyndigheten där de behandlas i brottsförebyggande eller brottsbekämpande syfte – i sådana fall måste det finnas rättsliga möjligheter att gå från sådan behandling till behandling enligt dataskyddsförordningen.

Det finns rättsligt stöd för nödvändig personuppgiftsbehandling

Dataskyddsförordningen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund (artikel 6). Den behandling av personuppgifter som myndigheter utför görs huvudsakligen med stöd av de rättsliga grunder som kommer till uttryck i artikel 6.1 c eller e, och som enligt artikel 6.3 ska fastställas i enlighet med unionsrätten eller nationell rätt. Den rättsliga

grunden enligt artikel 6.1 c innebär att behandlingen är laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Begreppet omfattar i första hand offentligrättsliga förpliktelser. Av 2 kap. 1 § dataskyddslagen följer att en förpliktelse utgör en rättslig grund för behandling av personuppgifter om förpliktelsen följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Den rättsliga grunden enligt artikel 6.1 e innebär att behandlingen är laglig om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. All verksamhet som en myndighet bedriver, inom ramen för sin befogenhet, anses vara av allmänt intresse (prop. 2017/18:105 s. 56–59). Av 2 kap. 2 § 1 dataskyddslagen följer att en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning utgör en rättslig grund för behandling av personuppgifter.

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

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

känsliga personuppgifter får behandlas av en myndighet med stöd av nämnda artikel om behandlingen är nödvändig för handläggningen av ett ärende. Detta innebär att det finns rättsligt stöd för Polismyndighetens behandling av känsliga personuppgifter i den mån sådana är relevanta för ett ärende enligt den nya lagen.

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

Detta betyder att det finns rättsligt stöd för den personuppgiftsbehandling som Polismyndigheten behöver vidta inom ramen för ett ärende enligt den nya lagen.

Som framgått kommer vissa personuppgifter i ärenden enligt den nya lagen att härröra från verksamheter vid Polismyndigheten där de behandlas i brottsförebyggande eller brottsbekämpande syfte, dvs. inom tillämpningsområdena för brottsdatalagen. Som noterats ovan måste det därför även finnas rättsliga möjligheter att gå från sådan behandling till behandling enligt dataskyddsförordningen. Enligt 2 kap. 22 § brottsdatalagen ska det, innan uppgifter behandlas för ett ändamål utanför den lagens tillämpningsområde, säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet, såvida skyldighet att lämna uppgifterna inte följer av lag eller förordning. En bedömning enligt 2 kap. 22 § måste alltså göras innan uppgifter kan överlämnas från Polismyndighetens brottsförebyggande och brottsbekämpande verksamheter till den del som handlägger ärenden enligt den nya lagen. I de fall uppgifterna är sådana att de kan behövas i ett ärende enligt den nya lagen kommer proportionalitetskravet, med hänsyn till vikten av en ändamålsenlig handläggning av sådana ärenden, emellertid i regel att vara uppfyllt. Det finns därför tillräckliga rättsliga möjligheter till sådana överlämnanden redan enligt befintlig reglering.

Den nya lagen innebär att värdtjänstleverantörer i sex månader ska bevara det rekryteringsinnehåll som har avlägsnats eller gjorts oåtkomligt, samt tillhörande data. Delar av det bevarade materialet kommer att innehålla personuppgifter. Rättslig grund för leverantörens behandling av sådana uppgifter under bevarandetiden finns i artikel 6.1 c i dataskyddsförordningen, eftersom den är

nödvändig för att fullgöra leverantörens rättsliga förpliktelse att bevara materialet. Rekryteringsinnehållet kan vidare, såsom anges ovan, innefatta känsliga personuppgifter enligt dataskyddsförordningen. Kravet på bevarande motiveras av att uppgifterna är nödvändiga antingen för vissa rättsliga förfaranden eller för brottsbekämpningsändamål. I båda fallen måste behandlingen anses ske för sådana viktiga allmänna intressen som innebär att den är tillåten enligt artikel 9.2 g, och i det förra fallet kan stöd dessutom finnas i artikel 9.2 f (om behandling för rättsliga anspråk). Rekryteringsinnehållet kan även innefatta personuppgifter som rör lagöverträdelser, vilket enligt artikel 10 i dataskyddsförordningen kräver att behandlingen är tillåten enligt unionsrätten eller nationell rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Bevarandeskyldigheten enligt den nya lagen innebär att behandlingen är tillåten enligt svensk rätt. Förutom de skyddsåtgärder som följer redan av dataskyddsförordningen och dataskyddslagen innebär den nya lagen dessutom att skyldigheten att bevara de aktuella personuppgifterna endast inträder när Polismyndigheten, efter en i lag reglerad prövning, utfärdar ett föreläggande om avlägsnande – som den enskilde kan överklaga om han eller hon anser det vara felaktigt. Sammantaget innebär detta att det finns lämpliga skyddsåtgärder enligt artikel 10, varför även behandlingen av personuppgifter som rör lagöverträdelser är tillåten.

Det finns inte behov av några kompletterande dataskyddsbestämmelser

För personuppgifter som behandlas vid Polismyndigheten i brottsförebyggande eller brottsbekämpande syfte finns särskilda bestämmelser om exempelvis längsta tid för behandling, särskilda upplysningar och tillgång till uppgifterna i brottsdatalagen och polisens brottsdatalag. Även dataskyddsförordningen innehåller en mängd bestämmelser till skydd för den vars personuppgifter behandlas med stöd av förordningen. Av de allmänna principerna för behandling av personuppgifter i artikel 5 följer bl.a. att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (ändamålsbegränsning), vara adekvata, relevanta och inte för omfattande i förhållande till de

ändamål för vilka de behandlas(uppgiftsminimering) och inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (s.k. lagringsminimering). Vid behandling av känsliga personuppgifter med stöd av artikel 9.2 g uppställer dataskyddsförordningen även ett krav på lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. En sådan åtgärd är den sökbegränsning som gäller enligt 3 kap. 3 § andra stycket dataskyddslagen. Detsamma gäller den sekretess som föreslås gälla till skydd för uppgifter om en enskilds personliga eller ekonomiska förhållanden i ärenden enligt den nya lagen (se avsnitt 8.1). Dessa bestämmelser motsvarar visserligen inte i alla delar vad som gäller enligt brottsdatalagen och polisens brottsdatalag, men innebär att det finns ett tillräckligt skydd för de enskilda vars personuppgifter kan komma att behandlas i ärenden enligt den nya lagen. Det finns därför inte behov av några kompletterande dataskyddsbestämmelser.

9 Överklagande

Förslag

Den behöriga myndighetens beslut ska få överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Skälen för förslaget

Det bör finnas en möjlighet att överklaga beslut om förelägganden och sanktionsavgifter till domstol. Om inte annat anges gäller att en förvaltningsmyndighets beslut kan överklagas till allmän förvaltningsdomstol (40 § förvaltningslagen). Det finns inte skäl att frångå denna ordning när det gäller beslut som den behöriga myndigheten fattar enligt den nya lagen, även om myndigheten kommer behöva göra vissa bedömningar som angränsar till straffrätten.

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

Ett beslut får överklagas av den som beslutet angår, om det har gått honom eller henne emot (42 § förvaltningslagen). Det innebär att en värdtjänstleverantör som mottagit ett föreläggande om avlägsnande eller annat beslut som fattats av den behöriga myndigheten med stöd av lagen kan ha rätt att överklaga det, liksom den vars innehåll berörs av ett sådant beslut.

10 Ikraftträdande- och övergångsbestämmelser

Förslag

Den nya lagen och lagändringarna ska träda i kraft den 1 september 2026.

Bedömning

Det finns inte behov av övergångsbestämmelser.

Skälen för förslaget och bedömningen

Lagförslagen syftar till att förhindra och försvåra onlinerekrytering och det är angeläget att reglerna kan träda i kraft så snart som möjligt. Det bedöms kunna ske den 1 september 2026.

Det bedöms inte finnas något behov av övergångsbestämmelser till den nya regleringen.

11 Konsekvenser

Bedömning

Förslagen ger inte upphov till några kostnader för berörda myndigheter som inte kan hanteras inom befintliga ekonomiska anslag.

Förslagen kan medföra begränsade kostnader och administrativa bördor för de företag som är värdtjänstleverantörer enligt förordningen om digitala tjänster.

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

Skälen för bedömningen

Ekonomiska konsekvenser för det allmänna

Förslagen innebär att Polismyndigheten som behörig myndighet ges möjlighet att besluta förelägganden om avlägsnade av rekryteringsinnehåll och om sanktionsavgifter i ärenden enligt den nya lagen. Sådan verksamhet kan inte bedrivas utan kostnader. Polismyndigheten uppskattar att det kan bli fråga om ett relativt stort antal ärenden per år och att antalet på sikt kan öka beroende på möjligheterna att automatisera delar av arbetet med att upptäcka rekryteringsinnehåll. Myndigheten har också påtalat att det kommer att krävas resurser för att omhänderta det rekryteringsinnehåll som upptäcks och för uppföljning av förelägganden och sanktionsärenden. Polismyndigheten har inrättat en Internet Referral Unit (IRU) som ansvarar både för att utfärda avlägsnandeordrar enligt TCO-förordningen och för de frivilliga mekanismer som finns för anmälan till onlineföretag av olagligt innehåll, bl.a. sådant rekryteringsinnehåll som kommer att omfattas av den nya lagen. Det

nuvarande systemet för anmälan är EU-gemensamt och framtaget för att användas i TCO-ärenden, men kan även användas för att skicka frivilliga förfrågningar till plattformar. Polismyndigheten har uppmärksammat Europol, som har hand om systemet, på behovet av att anpassa systemet även för förelägganden enligt artikel 9 i förordningen om digitala tjänster. I avvaktan på detta kan Polismyndigheten behöva skapa ett motsvarande system och utveckla interna metoder för att hantera förelägganden enligt den nya lagen.

Att Polismyndigheten ges rättsliga möjligheter att besluta förelägganden om avlägsnande kommer alltså innebära vissa kostnadsökningar för myndigheten. Kostnadsökningarna kan dock inte förväntas vara större än att de ryms inom ramen för myndighetens befintliga ekonomiska anslag.

Beslut enligt den nya lagen får överklagas till allmän förvaltningsdomstol. Det bedöms röra sig om ett mycket begränsat antal mål per år. Även för förvaltningsdomstolarnas del kan eventuella kostnadsökningar därför hanteras inom befintligt ekonomiskt anslag.

Obetalda sanktionsavgifter ska lämnas till Kronofogdemyndigheten för indrivning. Antalet sådana mål förväntas bli mycket begränsat och eventuella ökade kostnader för Kronofogdemyndigheten med anledning av förslagen kan hanteras inom befintligt ekonomiskt anslag.

När ett föreläggande om avlägsnande beslutas ska föreläggandet enligt förordningen om digitala tjänster även skickas till den myndighet som utsetts till samordnare för digitala tjänster, dvs. Post- och telestyrelsen, som sedan har att vidarebefordra det till andra samordnare för digitala tjänster inom unionen. Den hantering som detta kräver av Post- och telestyrelsen får förväntas bli begränsad. Detsamma gäller den förväntade effekten på myndigheten i dess egenskap av tillsynsmyndighet enligt förordningen om digitala tjänster. Även för Post- och telestyrelsens del kan eventuella kostnadsökningar därför hanteras inom befintligt ekonomiskt anslag.

Konsekvenser för företag

Förslagen innebär att de företag som är värdtjänstleverantörer och som omfattas av förordningen om digitala tjänster kan bli skyldiga att inom en timme avlägsna visst rekryteringsinnehåll eller göra det oåtkomligt samt att bevara vissa tillhörande data. En motsvarande skyldighet finns redan enligt TCO-förordningen beträffande terrorisminnehåll. Värdtjänstleverantörer är också skyldiga att ha mekanismer för hantering av anmälningar om olagligt innehåll enligt artikel 16 i förordningen om digitala tjänster. Den värdtjänst som mottar ett föreläggande om avlägsnande är också skyldig att informera den berörda tjänstemottagaren om det mottagna föreläggandet och den verkan det givits i enlighet med artikel 9.5 i förordningen om digitala tjänster. De skyldigheter som tillkommer med anledning av den nya lagen om avlägsnade av rekryteringsinnehåll bör inte kräva mer än en begränsad insats och bör därför innebära endast begränsade ekonomiska konsekvenser för de berörda företagen. Även den ökade administrativa bördan bör vara begränsad. Med hänsyn till de tungt vägande skälen bakom förslaget är intrånget i aktuella näringsverksamheter proportionerligt. De begränsade kostnaderna och administrativa bördorna ska bäras av de aktuella värdtjänstleverantörerna själva.

Konsekvenser ur ett rättighetsperspektiv

Den nya lagen syftar till att motverka spridning av vissa yttranden och annan information. Förslagen inverkar alltså på yttrande- och informationsfriheten. Som konstateras i avsnitt 6.1 är regleringen emellertid inte tillämplig på innehåll som skyddas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. I samma avsnitt bedöms att regleringen utgör en godtagbar begränsning av yttrande- och informationsfriheten enligt såväl regeringsformen som Europakonventionen och EU:s rättighetsstadga. Den inverkan som förslagen får på yttrande- och informationsfriheten är alltså proportionerlig i förhållande till de mål som avses uppnås.

Polismyndigheten kommer inom ramen för ärenden enligt den nya lagen att behöva behandla uppgifter om enskilda som kan vara känsliga av olika skäl. Det integritetsingrepp som detta innebär är nödvändigt för att uppfylla lagens bestämmelser och måste anses

godtagbart, inte minst med hänsyn till den sekretessbestämmelse till skydd för enskilda som föreslås.

Övriga konsekvenser

Förslagen kommer göra det möjligt för Polismyndigheten att i fler fall än i dag få bort rekryteringsinnehåll online, eller i vart fall göra det oåtkomligt. Dessutom kommer processen från det att innehållet upptäcks till dess att det tas bort eller görs oåtkomligt att gå snabbare än med dagens system som bygger på frivilliga åtgärder. Därmed ökar möjligheterna att förhindra att framför allt barn och unga rekryteras till att utföra brott och att avbryta pågående kontakter mellan en rekryterare och en potentiell utförare. Förslagen kan således förväntas få positiva effekter både för det brottsförebyggande och det brottsbekämpande arbetet. Förslagen förväntas även att få viss påverkan på jämställdheten eftersom majoriteten av de barn och unga som rekryteras är pojkar och unga män.

Förslagen bedöms inte ha någon betydelse för den kommunala självstyrelsen, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för möjligheterna att nå de integrationspolitiska målen eller påverka Sveriges åtaganden till följd av medlemskapet i Europeiska unionen.

12 Författningskommentar

12.1 Förslaget till lag om avlägsnande av rekryteringsinnehåll online

Lagens tillämpningsområde

1 § Denna lag reglerar förutsättningarna för att avlägsna innehåll som syftar till att rekrytera personer för att begå brott.

Paragrafen anger att lagen reglerar förutsättningarna för att avlägsna innehåll som syftar till att rekrytera personer för att begå brott. Övervägandena finns i avsnitt 4.1.

Vilket innehåll som omfattas av lagens tillämpningsområde framgår av 2–4 §§.

2 § Lagen gäller rekryteringsinnehåll som sprids till allmänheten online.

Med rekryteringsinnehåll avses innehåll som skäligen kan antas utgöra ett led i

1. straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer, eller
2. involverande av en underårig i brottslighet enligt 16 kap. 5 a § brottsbalken.

Paragrafen reglerar vad som avses med rekryteringsinnehåll. Övervägandena finns i avsnitt 4.2.

Enligt *första stycket* gäller lagen rekryteringsinnehåll som sprids till allmänheten online. Lagen är alltså begränsad till onlineinnehåll, dvs. innehåll som sprids till allmänheten via internet. Med att innehållet sprids till allmänheten avses att innehållet görs tillgängligt för ett potentiellt obegränsat antal personer, oberoende av hur många som faktiskt tar del av det. Även sådant innehåll som endast

är åtkomligt för personer som t.ex. har ett konto på en viss social medieplattform eller liknande anses spritt till allmänheten, förutsatt att det i princip är möjligt för var och en att registrera ett sådant konto. Detsamma gäller innehåll som sprids i t.ex. en chattgrupp. Innehåll som delas t.ex. i privata chattar mellan enskilda individer och i e-postmeddelanden faller däremot utanför tillämpningsområdet för lagen.

I *andra stycket* definieras vad som avses med rekryteringsinnehåll. Enligt *första punkten* krävs att innehållet är sådant att det skäligen kan antas att innehållet utgör ett led i en straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer. Detta innebär att det i straffskalan upptagna maximistraffet ska uppgå till minst två års fängelse. Det som är avgörande är den straffskala som är föreskriven för det brott som rekryteringen avser. Vidare krävs att brottet är straffbart på förberedelse- eller stämplingsstadiet.

Enligt *andra punkten* avses med rekryteringsinnehåll också innehåll som skäligen kan antas utgöra ett led i involverande av en underårig i brottslighet enligt 16 kap. 5 a § brottsbalken. När det gäller denna punkt uppställs det inte något krav på att det ska vara fråga om rekrytering till brottslighet av viss allvarlighetsgrad. Den straffbara gärningen enligt 16 kap. 5 a § brottsbalken består i att för brott eller brottslig verksamhet anlita, betala, instruera eller överlämna egendom till någon som är under 18 år, och därigenom, eller på annat liknande sätt, involvera honom eller henne i brottet eller den brottsliga verksamheten. För straffansvar krävs att gärningspersonens handlande innebär att den unge involveras i brott eller brottslig verksamhet. I detta krav ligger att den unges inblandning avser en brottslighet som någon annan i huvudsak står bakom.

Beviskravet, skäligen kan antas, innebär att det i det enskilda fallet ska finnas någon konkret omständighet som med viss styrka tyder på att innehållet utgör ett led i en straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer eller involverande av en underårig i brottslighet. När det gäller bedömningen av om det är fråga om att involvera en underårig i brottslighet är det tillräckligt att det framgår av sammanhanget att innehållet riktat sig till eller varit tillgängligt för personer under 18 år, t.ex. genom utformningen av innehållet eller genom att det har

publicerats på en plattform som används av minderåriga, och att det finns någon konkret omständighet som med viss styrka tyder på att någon har åtagit sig att utföra gärningen eller på annat sätt hörsammat uppmaningen och att denne är under 18 år.

Om beviskravet är uppfyllt i det enskilda fallet ska bedömas utifrån en helhetsbedömning med beaktande av innehållet i sig, dess kontext, var innehållet publicerats, vem som är avsändare, mottagarkretsen etc. Vid denna bedömning kan flera inlägg som publicerats i en följd eller på annat sätt i ett sammanhang behöva bedömas gemensamt.

Även innehåll som i praktiken lett till en fullbordad anstiftan omfattas och kan bli föremål för ett föreläggande om avlägsnande förutsatt att brottet är straffbart på förberedelse- eller stämplingsstadiet eller avser rekrytering av en underårig.

3 § Lagen gäller endast rekryteringsinnehåll som riktar sig till personer i Sverige eller avser brott som ska begås här eller mot en svensk medborgare eller någon som har hemvist i Sverige.

Paragrafen reglerar att lagen endast gäller rekryteringsinnehåll som har anknytning till Sverige. Övervägandena finns i avsnitt 4.3.

I paragrafen anges att lagen endast gäller rekryteringsinnehåll som riktar sig till personer i Sverige eller avser brott som ska begås här eller mot en svensk medborgare eller någon annan som har hemvist i Sverige. Ett föreläggande om avlägsnande enligt 5 § kan alltså beslutas både beträffande innehåll som avser rekrytering av svenskar till brott och innehåll som syftar till att rekrytera andra än svenskar för att begå brott här i landet eller mot en svensk person. Med medborgare eller annan som har hemvist här avses detsamma som i 2 kap. 3 § brottsbalken.

För att bedöma om kravet att innehållet är riktat till personer i Sverige är uppfyllt ska en helhetsbedömning göras utifrån innehållet som sådant och dess kontext, var det publicerats etc. Enbart teknisk åtkomst till innehåll som publiceras online är inte tillräckligt. Kravet bör däremot normalt anses uppfyllt om innehållet publiceras på en plattform eller domän med tydlig anknytning till Sverige. Även innehåll som inte riktar sig till personer i Sverige kan omfattas om det t.ex. av innehållet som sådant eller av dess sammanhang framgår

att det är fråga om rekrytering till ett brott som planeras att utföras i Sverige eller mot en svensk person.

4 § Lagen gäller inte innehåll som omfattas av Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online.

I paragrafen anges undantag från lagens tillämpningsområde. Övervägandena finns i avsnitt 4.4.

I paragrafen anges att lagen inte gäller innehåll som omfattas av TCO-förordningen, dvs. terrorisminnehåll. Vad som avses med terrorisminnehåll anges i artikel 2.7 i förordningen. I sådana fall ska i stället förordningens bestämmelser och den kompletterande TCO-lagen tillämpas på innehållet.

Föreläggande att avlägsna rekryteringsinnehåll

5 § Den myndighet regeringen bestämmer (den behöriga myndigheten) får förelägga en värdtjänstleverantör att avlägsna rekryteringsinnehåll.

Med värdtjänstleverantör avses en sådan leverantör av värdtjänster som omfattas av Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

Paragrafen ger den behöriga myndigheten möjlighet att besluta om föreläggande om avlägsnande av rekryteringsinnehåll. Övervägandena finns i avsnitt 5.1.

I *första stycket* anges att regeringen bestämmer vilken myndighet som är behörig myndighet enligt lagen. Vidare anges i första stycket att den behöriga myndigheten får förelägga en värdtjänstleverantör att avlägsna rekryteringsinnehåll. Vad som avses med rekryteringsinnehåll framgår av 2 § (se kommentaren till den bestämmelsen). Samtliga förutsättningar i 2 och 3 §§ behöver vara uppfyllda för att ett föreläggande ska kunna utfärdas. Detta innebär bl.a. att innehållet ska ha spritts till allmänheten online, att det skäligen kan antas att innehållet utgör ett led i en straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer eller involverande av en underårig i brottslighet och att innehållet har anknytning till Sverige. Om förutsättningarna är uppfyllda får

bedömas utifrån en helhetsbedömning av innehållet som sådant och dess kontext, var det publicerats, mottagarkretsen etc.

I *andra stycket* anges att med värdtjänstleverantör avser en sådan leverantör av värdtjänster som omfattas av EU:s förordning om digitala tjänster. Hänvisningen till förordningen innebär dels att förordningens definition av vad som avses med en värdtjänst gäller, dels att lagen gäller sådana värdtjänster som omfattas av förordningen. Det innebär bl.a. att det krävs att värdtjänstleverantören erbjuder tjänster i unionen och att värdtjänsten har väsentlig anknytning till unionen. Att en webbplats är tekniskt åtkomlig i unionen är inte tillräckligt. Hänvisningen till förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

6 § Föreläggandet ska uppfylla de krav som följer av artikel 9.2 i förordningen om digitala tjänster.

I artikel 9 i förordningen om digitala tjänster finns bestämmelser om förfarandet efter beslut om ett sådant föreläggande.

Paragrafen reglerar hur ett föreläggande ska utformas. Övervägandena finns i avsnitt 5.2.

Enligt *första stycket* ska ett föreläggande om att avlägsna rekryteringsinnehåll enligt 5 § uppfylla de krav som följer av artikel 9.2 i förordningen om digitala tjänster. Bestämmelserna i förordningen reglerar vissa krav på innehåll och förfarande i de fall ett föreläggande mot en leverantör av en förmedlingstjänst, i detta fall en värdtjänst, beslutas med stöd av annan unionsrätt eller nationell lagstiftning.

Andra stycket upplyser om att det i artikel 9 i förordningen om digitala tjänster finns bestämmelser om förfarandet efter beslut om ett föreläggande.

Hänvisningarna till förordningen är dynamiska. Det innebär att de avser förordningen i den vid varje tidpunkt gällande lydelsen.

7 § Den värdtjänstleverantör som mottar ett föreläggande ska avlägsna rekryteringsinnehållet eller göra det oåtkomligt så snart som möjligt och senast inom en timme från mottagandet av föreläggandet.

Om det är tillräckligt att innehållet görs oåtkomligt i en eller flera stater ska den behöriga myndigheten ange det i föreläggandet.

Paragrafen innehåller regler om värdtjänstleverantörens skyldighet att avlägsna rekryteringsinnehåll eller göra det oåtkomligt. Övervägandena finns i avsnitt 5.3.

I *första stycket* anges att den värdtjänstleverantör som mottar föreläggandet ska avlägsna rekryteringsinnehållet eller göra det oåtkomligt så snart som möjligt och senast inom en timme från mottagandet av föreläggandet. Skyldigheten att göra innehållet oåtkomligt gäller utan begränsning till visst territoriellt område. Ett undantag från detta finns i andra stycket.

Om det är tillräckligt att innehållet görs oåtkomligt i en eller flera stater ska, enligt *andra stycket*, den behöriga myndigheten ange det i föreläggandet. Det kan i vissa fall vara tillräckligt att innehållet görs oåtkomligt t.ex. i Sverige eller i vissa nordiska länder. Det ankommer på den behöriga myndigheten att bedöma vilket behov som finns i det enskilda fallet.

En överträdelse av skyldigheterna i paragrafen kan leda till sanktionsavgift (se 9 §).

Bevarande av rekryteringsinnehåll

8 § En värdtjänstleverantör ska bevara det rekryteringsinnehåll, samt tillhörande data, som har avlägsnats eller gjorts oåtkomligt till följd av ett föreläggande.

Rekryteringsinnehållet och tillhörande data ska bevaras i sex månader från det att innehållet avlägsnats eller gjorts oåtkomligt.

Paragrafen innehåller bestämmelser om skyldighet för värdtjänstleverantör att bevara visst innehåll. Övervägandena finns i avsnitt 5.4.

Enligt *första stycket* ska en värdtjänstleverantör bevara det rekryteringsinnehåll som har avlägsnats eller gjorts oåtkomligt till följd av ett föreläggande om avlägsnande, samt tillhörande data. Med tillhörande data avses uppgifter som exempelvis identitet och IP-adress för den som publicerat innehållet samt datum och tidpunkt för publiceringen.

I *andra stycket* anges att kravet på bevarande gäller i sex månader från det att värdtjänstleverantören avlägsnade rekryteringsinnehållet eller gjorde det oåtkomligt.

En överträdelse av skyldigheterna i paragrafen kan leda till sanktionsavgift (se 9 §).

Sanktionsavgifter

9 § Den behöriga myndigheten får besluta att ta ut en sanktionsavgift av en värdtjänstleverantör som överträder någon av sina skyldigheter enligt 7 och 8 §§.

Paragrafen ger den behöriga myndigheten möjlighet att besluta om uttagande av sanktionsavgift av en värdtjänstleverantör som åsidosätter vissa skyldigheter enligt lagen. Övervägandena finns i avsnitt 7.1.

Paragrafen innebär att den behöriga myndigheten får besluta att ta ut en sanktionsavgift vid överträdelse av skyldigheten att avlägsna eller göra rekryteringsinnehåll oåtkomligt så snart som möjligt och senast inom en timme från mottagandet av en avlägsnandeorder (7 §) eller skyldigheten att bevara rekryteringsinnehåll och tillhörande data (8 §).

Värdtjänstleverantörens ansvar är strikt. Det krävs alltså varken uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut, utan det är tillräckligt att ett åsidosättande har skett. Det är den behöriga myndigheten som avgör om det finns skäl att ta ut en sanktionsavgift.

10 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och högst 5 000 000 kronor eller, vid en systematisk eller fortgående underlåtenhet att fullgöra skyldigheten enligt 7 §, upp till ett sådant högre belopp som motsvarar fyra procent av leverantörens globala omsättning närmast föregående räkenskapsår.

Om en överträdelse som kan leda till högre sanktionsavgift än 5 000 000 kronor har skett under leverantörens första verksamhetsår eller om uppgifter om omsättningen annars saknas eller är bristfälliga, får omsättningen uppskattas.

Paragrafen reglerar vilka belopp som sanktionsavgiften ska bestämmas till. Övervägandena finns i avsnitt 7.2.

I *första stycket* fastställs det lägsta och det högsta beloppet för en sanktionsavgift. När det är fråga om en systematisk eller fortgående underlåtenhet att fullgöra skyldigheten enligt 7 § – dvs. skyldigheten

att avlägsna eller göra rekryteringsinnehåll oåtkomligt – gäller en särskild regel för bestämmandet av det högsta tillåtna beloppet. Detta får då uppgå till maximalt fyra procent av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret, om denna summa överstiger 5 000 000 kr. När sanktionsavgiftens storlek ska bestämmas måste en helhetsbedömning göras. Särskild hänsyn kan då tas till exempelvis hur allvarlig överträdelsen är samt leverantörens finansiella ställning.

När överträdelsen är sådan att sanktionsavgiften kan bestämmas till högre belopp än 5 000 000 kr får leverantörens omsättning enligt *andra stycket* under vissa förhållanden uppskattas. Detta gäller om sanktionsavgift påförs under värdtjänstleverantörens första verksamhetsår, eftersom det då inte finns några tidigare verksamhetsår att jämföra med. Omsättningen får uppskattas även om överträdelsen inte har skett under det första verksamhetsåret, om tillförlitlig uppgift om omsättningen under det närmast föregående räkenskapsåret saknas. En uppskattning av omsättningen bör göras med försiktighet.

11 § Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna framstår som oskäligt att ta ut avgiften.

Paragrafen reglerar under vilka förhållanden den behöriga myndigheten får sätta ned sanktionsavgiften. Övervägandena finns i avsnitt 7.2.

Av paragrafen framgår att den behöriga myndigheten under vissa förhållanden får sätta ner sanktionsavgiften, helt eller delvis. Detta gäller om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna framstår som oskäligt att ta ut avgiften. Eftersom värdtjänstleverantörens ansvar är strikt kan det t.ex. vara fråga om ett avlägsnande som tagit något längre tid än en timme och där tidsutdräkten av exempelvis tekniska skäl inte kan läggas leverantören till last. Det kan också finnas skäl att avstå från att ta ut sanktionsavgift för att förbudet mot dubbelprövning annars skulle förhindra ett brottmålsförfarande mot värdtjänstleverantören.

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

Ett beslut om sanktionsavgift ska delges.

Paragrafen reglerar bl.a. preskriptionstiden för beslut om sanktionsavgift. Övervägandena finns i avsnitt 7.3.

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

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

Betalning av sanktionsavgifter

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

Sanktionsavgiften tillfaller staten.

Paragrafen reglerar betalning av sanktionsavgifter. Övervägandena finns i avsnitt 7.3.

Första stycket anger till vem och när en sanktionsavgift ska betalas. Om avgiften inte betalas inom den angivna tiden, ska den behöriga myndigheten lämna den obetalda avgiften för indrivning enligt lagen (1993:891) om indrivning av statliga fordringar m.m. Beslutet om sanktionsavgift utgör en exekutionstitel (3 kap. 1 § första stycket 6 utsökningsbalken). Det innebär att verkställighet enligt utsökningsbalken kan ske utan att det krävs något domstolsavgörande.

Enligt *andra stycket* tillfaller sanktionsavgiften staten.

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

Paragrafen reglerar preskription av sanktionsavgifter. Övervägandena finns i avsnitt 7.3.

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

Överklagande

15 § Den behöriga myndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

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

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

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

Rätt att meddela föreskrifter

16 § Regeringen eller den myndighet regeringen bestämmer får meddela ytterligare föreskrifter om informationsskyldigheten enligt artikel 9.5 i förordningen om digitala tjänster.

I paragrafen bemyndigas regeringen eller den myndighet regeringen bestämmer att meddela föreskrifter om informationsskyldigheten enligt artikel 9.5 i förordningen om digitala tjänster. Övervägandena finns i avsnitt 5.2.

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

35 kap.

TCO-förordningen och lagen om avlägsnande av rekryteringsinnehåll online

23 c § Sekretess gäller hos Polismyndigheten för uppgift om en enskilds personliga eller ekonomiska förhållanden, *om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs och uppgiften förekommer* i ärende enligt

1. Europaparlamentets och rådets förordning (EU) 2021/784 av den 29 april 2021 om åtgärder mot spridning av terrorisminnehåll online och enligt lagen (2023:319) med kompletterande bestämmelser till EU:s förordning om åtgärder mot spridning av terrorisminnehåll online, *eller*

2. lagen (2026:000) om avlägsnande av rekryteringsinnehåll online.

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

Paragrafen reglerar sekretessen hos Polismyndigheten i ärenden enligt TCO-förordningen, TCO-lagen och lagen om avlägsnande av rekryteringsinnehåll online. Övervägandena finns i avsnitt 8.1.

I *första stycket* görs ett tillägg som innebär att det föreskrivs att sekretess gäller hos Polismyndigheten även för uppgift om en enskilds personliga eller ekonomiska förhållanden i ärende enligt lagen om avlägsnande av rekryteringsinnehåll online. Det kan exempelvis gälla uppgifter om enskildas kopplingar till kriminella nätverk eller om brott eller brottslig verksamhet. Dessutom kan skyddsvärda uppgifter om en värdtjänstleverantörs ekonomiska förhållanden behöva behandlas i ärenden som rör sanktionsavgifter.

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

Övriga ändringar i paragrafen är redaktionella.

Departementsserien 2026

Kronologisk förteckning

1. Nya möjligheter att bekämpa onlinerekrytering. Ju.

Departementsserien 2026

Systematisk förteckning

Justitiedepartementet

Nya möjligheter att bekämpa onlinerekrytering. [1]